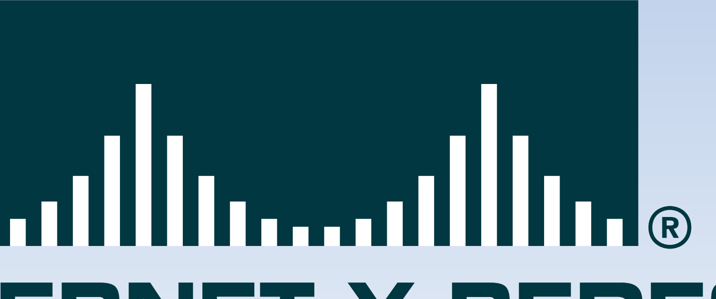
IPv6 ya!! | STORAGE | VoIP y Multicast | DATA centers

NEX IT SPECIALIST

PRECIO ARGENTINA $7 #19

NEX IT SPECIALIST - REVISTA DE NETWORKING Y PROGRAMACIÓN

CISCO SYSTEMS



INTERNET Y REDES INTELIGENTES

IP-NGN
Redes de Nueva Generación



Wireless
Convergencia Fija Móvil

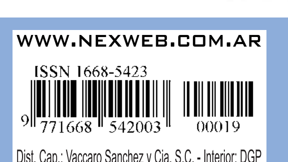
Innovación en
Networking IP

REDES
Auto-Defensivas



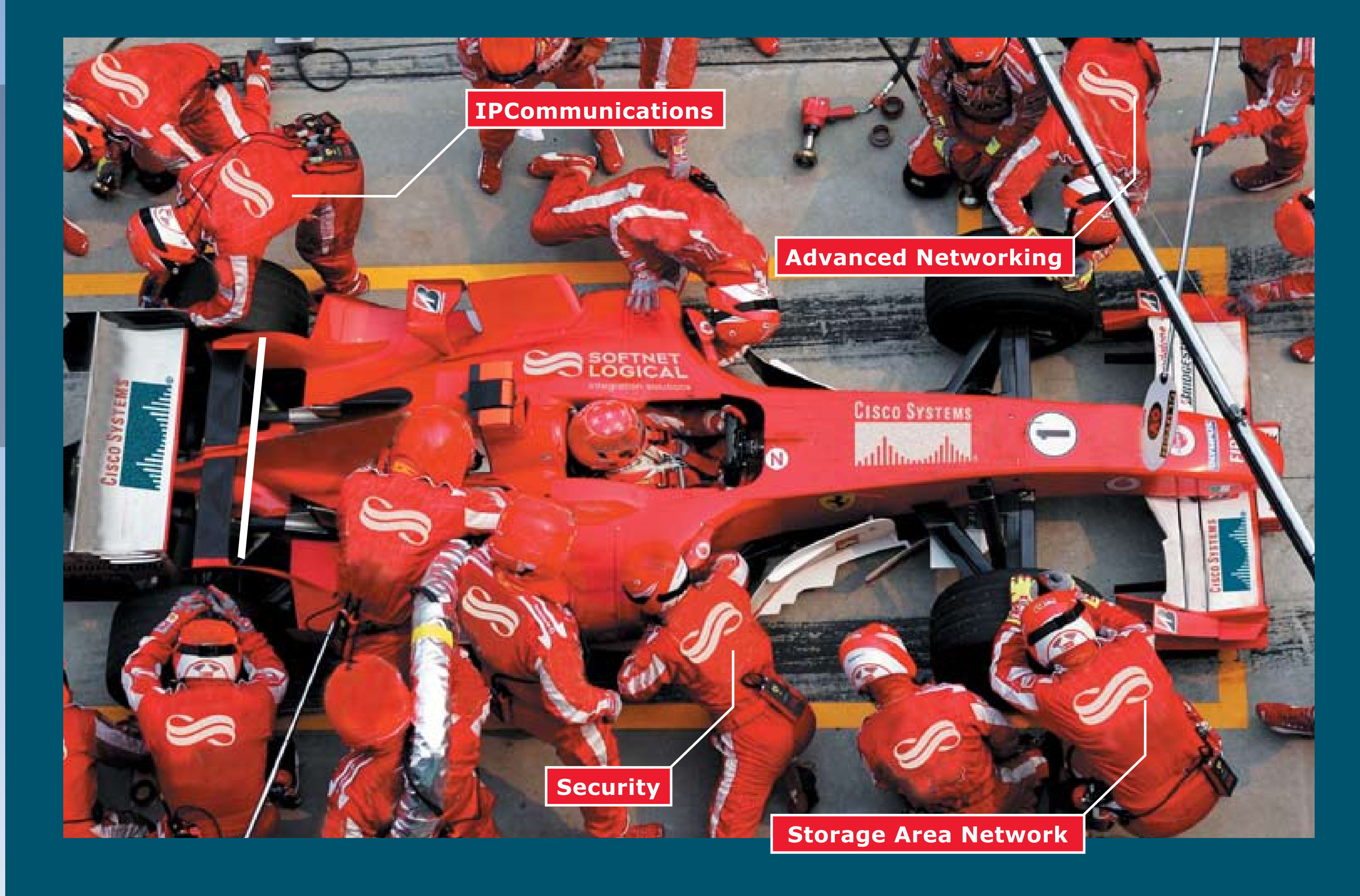


WWW.NEXWEB.COM.AR


ISSN 1668-5423

Dist. Cap.: Vaccaro Sanchez y Cia. S.C. - Interior: DGP

GUIA DE REFERENCIA RAPIDA DE PRODUCTOS CISCO



APPLIED TECHNOLOGIES

La tecnología del lado de su negocio



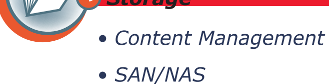
- Voice Aplications
- Contact Centers
- Unified Messaging



- Wireless
- Optical
- Last Mile



- Self Defending
- Intrusion Detection
- Aplications & Access



- Content Management
- SAN/NAS
- Knowledge Management

*Como proveedores de servicios, las respuestas que ofrecemos a nuestros clientes, están asociadas al concepto de solución, que no es más que la **tecnología aplicada a resolver situaciones de negocio.***

Descubra Softnet Logical, y sume a sus negocios la mejor tecnología y el mejor know-how en IT.

www.la.logicalis.com

+54 (11) 4344-0333
info@la.logicalis.com

Argentina +54 (11) 4344-0333 Uruguay +598 (2) 711-3333 Paraguay +595 (21) 230-041





RECERTIFICAMOS POR 7° AÑO
FEBRERO - 2005

solución de comunicaciones para la mediana empresa

Cisco ha diseñado una Solución de Comunicaciones inteligente, simple y segura, para empresas de tamaño mediano que buscan controlar costos, mejorar la eficiencia operativa y obtener una ventaja competitiva sostenible. La Solución de Comunicaciones de Cisco para empresas medianas provee la infraestructura y aplicaciones que su empresa necesita para potenciar sus negocios, como la nueva familia de switching Cisco Catalyst Express 500 Series y adiciones al portafolio de Comunicaciones IP.

Para más información, deje sus datos aquí
www.cisco.com/offer/solucionempresarial
o comuníquese al 0810-444-CISCO (24726)

innovation. powered by CISCO SYSTEMS®

© 2005 Cisco Systems, Inc. Todos los derechos reservados.



DIRECTOR
- Dr. Carlos Osvaldo Rodriguez

PROPIETARIOS
- Editorial Poulbert S.R.L.

COORDINADOR EDITORIAL
- Carlos Rodríguez Bontempi

RESPONSABLE DE CONTENIDOS
- Dr. Carlos Osvaldo Rodríguez

EDITORES
- Carlos Vaughn O'Connor
- Carlos Rodríguez

GERENCIA COMERCIAL
- Ulises Román Mauro
umauro@nexweb.com.ar

DISTRIBUCIÓN
- Mariano H. Agüero
distribucion@nexweb.com.ar

SUSCRIPCIONES
- Maximiliano Sala
suscripciones@nexweb.com.ar

DISEÑO Y COMUNICACIÓN VISUAL
- Esteban Báez
- Carlos Rodríguez Bontempi

PREIMPRESIÓN E IMPRESIÓN
Impresión: IPESA Magallanes 1315. Cap. Fed. Tel 4303-2305/10
Impresión de esta Edición 10.000 ejemplares

DISTRIBUCIÓN
Distribución en Capital Federal y Gran Buenos Aires: Vaccaro, Sánchez y Cia. S. C. Moreno 794, Piso 9. 1091- Capital Federal Argentina.
Distribuidora en Interior: DGP Distribuidora General de Publicaciones S.A. Alvarado 2118/56 1290 Capital Federal - Argentina
NEX IT Revista de Networking y Programación
Registro de la propiedad Intelectual en trámite leg número 3038 ISSN 1668-5423
Dirección: Av. Corrientes 531 P 1
C1043AAF - Capital Federal
Tel: +54 (11) 5031-2287

Queda prohibida la reproducción no autorizada total o parcial de los textos publicados, mapas, ilustraciones y gráficos incluidos en esta edición. La Dirección de esta publicación no se hace responsable de las opiniones en los artículos firmados, los mismos son responsabilidad de sus propios autores. Las notas publicadas en este medio no reemplazan la debida instrucción por parte de personas idóneas. La editorial no asume respon-sabilidad alguna por cualquier consecuencia, derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen, analizan o publican.

Si desea escribir para nosotros, enviar un e-mail a: articulos@nexweb.com.ar



Nota del Editor

El trabajar por cerca de dos meses en este ejemplar de "NEX IT Specialist", que está centrado en tecnologías Cisco, nos ha permitido rescatar dos aspectos de Cisco Systems: la profesionalidad de quienes lo forman y el espíritu innovador de la empresa.
Durante dos meses se nos ha permitido interactuar con sus ingenieros, expertos en prensa, marketing y directivos en un marco y con un espíritu semejante al de un ámbito académico. Tuvimos la sensación de estar trabajando en una universidad como Berkeley, el MIT o Cambridge en UK.
Es que Cisco nació en Stanford University (léase una de las mejores universidades del mundo) y aún refleja ese espíritu.
Cisco es líder y el único modo de serlo es a través de la "innovación". Cuando se habla de la importancia de la investigación científica /tecnológica de un país o empresa nos referimos a la capacidad de crear conocimiento original. Cisco ha sido pionera en muchas innovaciones que han cambiado no sólo el mundo de Networking sino también el de nuestra vida diaria. Y esto, sólo se logra teniendo gente de excelencia y volcando recursos y más recursos apostando a esa gente y a esas ideas originales.
Innovación en Cisco va de la mano de la creación de estándares que aseguran que los avances pueden ser usados por todo el mundo. Para ejemplificar esta breve editorial menciono solo algunos: Border Gateway Protocol (BGP), Dynamic Packet Transport/resilient Packet Ring (DPT/RPR), Multiprotocol Label Switching (MPLS) and Layer 2 Tunneling Protocol (L2TP).
Los artículos de "NEX IT Specialist" #19, están basados en tecnologías Cisco y sus productos, pero, hemos seleccionado un abanico de temas que le darán al lector una idea clara de a donde va el Networking del futuro.
Nos faltó espacio, hubiésemos querido ahondar desde conceptos básicos (innovaciones en IOS, MPLS, IPSec, L2TP…) hasta conocer que sucede con Internet en el espacio exterior. Estos artículos estaban listos pero la falta de lugar no nos permitió incluirlos. Búsquenlos en nuestros próximos NEX.
Y, no se pierdan "NEX IT Specialist" #20 que nuevamente estará dedicado a seguridad informática: "Ethical Hacking 3".

Para aquellos que no han tenido contacto con tecnologías y/o productos CISCO recomendamos leer primero los artículos en Pág. 12 (CISCO-IOS) y Pág. 15 (MPLS).

Cisco Systems



04

Cisco, un puente a la innovación

Sebastián Ballerini, Gerente General de Cisco Systems para Argentina dialogó con NEX IT Specialist sobre la actualidad y la visión a futuro de Cisco.

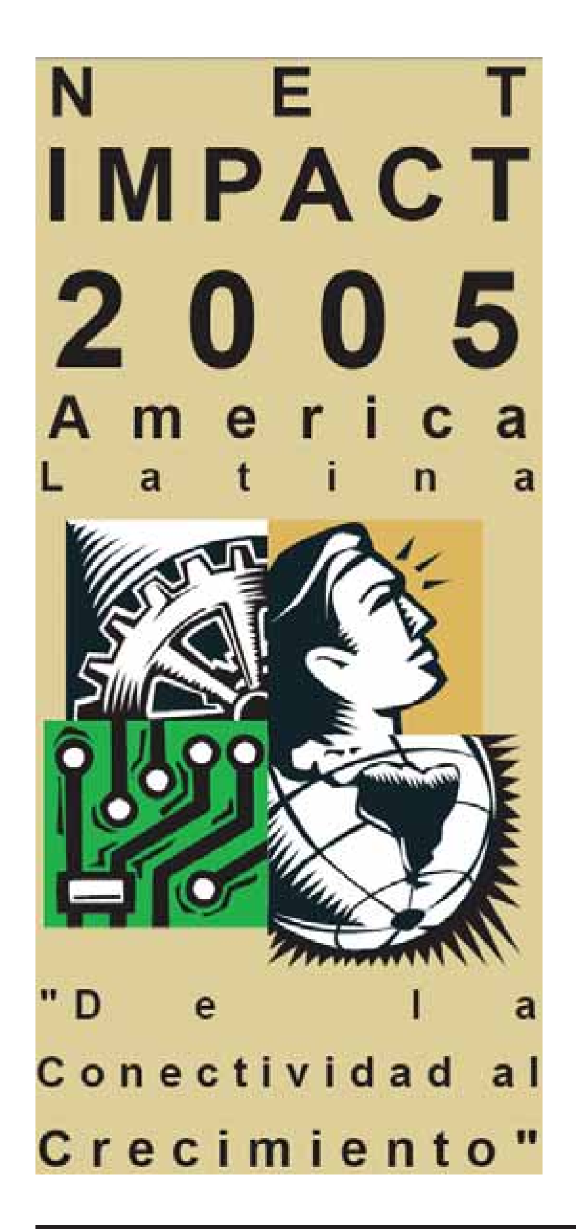
26

IP-NGN

La innovación de Cisco y sus avances en tecnología están ayudando a los proveedores de servicios en la transformación hacia las redes de la próxima generación basadas en IP.



Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.



La satisfacción del cliente y el deseo por mejorar la competitividad son los motivos principales por los cuales las organizaciones (empresas y gobiernos) invierten en tecnología en Latinoamérica, de acuerdo a un estudio presentado por el Instituto de Conectividad en las Américas (ICA, por sus siglas en inglés) y Cisco Systems.

El estudio, "Net Impact 2005 Latin America, From Connectivity to Growth" (Net Impact 2005 Latinoamérica, de la Conectividad al Crecimiento), encontró que un 52% de las compañías invierte en tecnología para incrementar la satisfacción del cliente, y un 46% lo hace para aumentar su competitividad.

Así mismo, que el 70% de las organizaciones en América Latina reporta que la tecnología les ha ayudado a incrementar la satisfacción del cliente en promedio en un 32%; un 45% de organizaciones ha visto una reducción en costos operativos en promedio en un 15% y un 32% de las organizaciones ha incrementado sus ingresos en promedio en un 11%.

El estudio también muestra que la infraestructura de banda ancha de las empresas Latinoamericanas y del sector público es inadecuada. Un 62% reporta un promedio de velocidad de conexión de 128-768 kbps y solo un 15% tiene E1 o conexiones mayores. Cerca de un 40% de las organizaciones de Estados Unidos (2003) reportaron un promedio de conexión de banda ancha de 1.5 megabits por segundo o de mayor capacidad.

El estudio, patrocinado por Cisco Systems, fue realizado por Momentum Research, e incluyó entrevistas a más de 1,200 ejecutivos que toman decisiones en materia de tecnología en México, Brasil, Costa Rica, Colombia, Chile y Argentina, del sector público (entidades de gobierno, salud y educación), retail, manufactura y servicios financieros.

CALENDARIO DE EVENTOS IT EN ARGENTINA

Fecha	OCTUBRE	Informes
19	**VI Jornada de Tecnologías de Internet** Sheraton Libertador, Buenos Aires	mgparra@worktec.com.ar Te. (5411) 4803-6100

Fecha	NOVIEMBRE	Informes
9 Y 10	**CONSECRI** Congreso de Seguridad y Criptografía Sheraton Libertador, Buenos Aires	mgparra@worktec.com.ar Te. (5411) 4803-6100
9 Y 10	**CONSETIC** Congreso Hispano - Lusoamericano de Seguridad Informática Sheraton Libertador, Buenos Aires	mgparra@worktec.com.ar Te. (5411) 4803-6100
20 al 23	**5º Jornadas Regionales de Software Libre** Cafferata 729, Ciudad de Rosario	www.jornadas.ant.org.ar info@jornadas.ant.org.ar
27	**TechNight Córdoba - Infraestructura** Introducción a Microsoft Virtual Server 2005. Hipólito Yrigoyen 146, Piso 14. Ciudad de Córdoba	http://msevents.microsoft.com/cui/EventDetail.aspx?culture=es-AR&EventID=1032283497&EventCategory=1
29	**Gira Nacional MUG y MSDN: SQL Server 2000 / 2005 Preview** Universidad Tecnológica Nacional - Facultad Regional Santa Fe	http://girainterior.mug.org.ar/
30	**Trabajo IT 2 – Versión 2.00.5 B** Sheraton Libertador, Buenos Aires	mgparra@worktec.com.ar Te. (5411) 4803-6100

Si desea ver su evento IT publicado en esta sección, por favor háganos llegar la información respectiva a: eventos@nexweb.com.ar



Cisco, un puente a la innovación

Autor: **David A. Yanover**
Director de www.mastermagazine.info

Sebastián Ballerini, Gerente General de Cisco Systems para Argentina dialogó con NEX IT Specialist sobre la actualidad y la visión a futuro de Cisco. Hacemos un viaje en el que impera la conectividad y el uso de las distintas formas de Internet.

Con 21 años próximos a cumplir en diciembre, Cisco es una empresa adulta, pero no por su edad, sino por su papel en el continuo avance tecnológico. Simbolizando y representando el espectro de las redes y la conectividad, pero abarcando también otras áreas con gran interés, como es el caso de la telefonía IP y Seguridad. Cisco lleva a recorrer un camino que tiene sus orígenes en la Universidad de Stanford, allá por el año 1984.

Para conocer las actividades de Cisco, NEX IT Specialist conversó en exclusiva con Sebastián Ballerini, Gerente General de Cisco Systems para Argentina, Bolivia, Paraguay y Uruguay. Al acceder a él, inmediatamente remarcó la relación de Cisco con el entorno educativo, y el hecho de que "la empresa nació de la nada, convirtiéndose veinte años des-

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.



pués en una compañía capaz de facturar 24 mil millones de dólares, reflejando un crecimiento de más del 13% anual, y teniendo hoy una presencia global".

Cisco comenzaba a decir sus primeros unos y ceros en diciembre de 1984, cuando era fundada por Len Bosack y Sandy Lerner, dos científicos de la Universidad de Stanford, que junto a otros colegas comenzaron a experimentar tratando de conectar edificios del campus académico, primero utilizando puentes y luego routers. De esta forma nace el primer producto de Cisco, un router capaz de soportar múltiples protocolos, de tal manera que ambas máquinas puedan hablarse entre sí. Oficialmente, es lanzado el subsistema MEIS.

Los significados del nombre y el logo de Cisco tienen sus propias particularidades. Por un lado, Cisco responde a una abreviación de la ciudad de San Francisco, mientras que la imagen de la empresa es divisada cuando la pareja de fundadores viajaba a Sacramento a registrarla, ya que durante el camino les llamó la atención ver cortada la imagen del puente Golden Gate por el reflejo del sol. Así lo atestigua John Morgridge, quien dirigió los años iniciales que vivió el rey del networking.

Recién hacia 1986, la empresa contrataría a su primer empleado. Hoy, según explica Ballerini, Cisco cuenta con más de 37 mil trabajadores, distribuidos en 300 sedes en 90 países. "En Argentina tenemos cien personas, una oficina en Buenos Aires y un modelo de venta indirecto. Tenemos un fuerte compromiso de trabajo con nuestros partners, brindándoles permanente acceso a herramientas de soporte, ventas, capacitación y demás aspectos que giran en torno a los productos".

En 1986, los primeros dominios .com y .edu era asignados, y existían más de dos mil hosts; hoy, comienzan a venderse sitios con denominación .xxx y más de 6.3 billones de personas navegan por la Web, según los datos de Internet World Stats, una consultora del tráfico que circula por la red. Al principio del período que se ha marcado, Cisco colaboró con el Internet Engineering Task Force (IETF), un organismo que analiza la arquitectura de Internet. Paralelamente, el novedoso router de Cisco, AGS (Advanced Getaway Server) rompió todos los parámetros de conectividad conocidos hasta aquél momento.

Un año después, Cisco desarrolló el Multiport Communications Interface, que logró altas velocidades estando constituido por dos puertos seriales y otros dos Ethernet.

En febrero del '90 la empresa decidió hacerse pública en la bolsa de Nasdaq, lo cual fue un movimiento trascendental que le permitió a Cisco el reconocimiento que buscaba. Declarada como una de las principales empresas en las listas de Fortune de aquél entonces, y cotizando US$ 224 millones, Cisco dejó de ser un nombre conocido sólo por el entorno tecnológico. En 1991 John Chambers, actual Presidente y CEO de Cisco Systems, se unió a la compañía Cisco como Vicepresidente Senior de Operaciones y Ventas a nivel mundial.

La explosión que sufrió Internet poco antes del nuevo milenio se convirtió en un impulso que hizo posible un rápido crecimiento de la empresa, y factor clave fue también la política en cuanto a la adquisición de compañías. Sólo en los últimos tres años, Cisco ha comprado veinte empresas, y uno de cada siete empleados proviene de las incorporaciones que se llevaron a cabo, las cuales cada vez se realizan con mayor intensidad. La lista de compras fue inaugurada en 1993, con Crescendo Communications, una firma dedicada a proveer productos de networking relacionados con el trabajo colaborativo. Es gracias a este modelo, que Cisco consigue ampliar drásticamente su mercado.

Más tarde, las cifras caerían significativamente, pero sin atarse a la crisis que sufrieron los sitios de Internet. Para Cisco, el negocio continuaba intacto. Y hoy la empresa es considerada por la prestigiosa revista Fortune como uno de los mejores lugares donde trabajar, ocupando en el 2005 el cuarto lugar, apareciendo entre los 25 principales por octava vez en la lista.

Soluciones e intereses

"La génesis de la compañía es el mercado corporativo. Sin embargo hoy tenemos un fuerte posicionamiento hacia las empresas más pequeñas. Es importante destacar que cuando en Cisco hablamos de soluciones para el mercado medio, no adaptamos las estructuras de redes o los productos para las grandes corporaciones a empresas más pequeñas. Tenemos un equipo dedicado a la integración de todas las tecnologías y al desarrollo de soluciones especialmente definidas de acuerdo a los requerimientos de las pymes que básicamente buscan en la tecnología una mejora en la competitividad, mayor eficiencia en el desarrollo de sus actividades, satisfacción de sus clientes y reducción en los costos de negocios". También, Ballerini explica el enfoque mediante el cual Cisco se presenta a sus clientes, a quienes muchas veces les cuesta interesarse en los aspectos técnicos, por lo que "compran el valor de la solución", es decir, el resutado que se obtiene tras la aplicación de la herramienta informática.

La empresa presenta actualmente cuatro modelos de negocios fundamentales. Por un lado, Enterprise, que consiste en el escalón de mayor nivel, donde son atendidas las principales empresas del país; luego, está la línea de Proveedores de Servicios, que en el caso de Argentina, figuran compañías tales como Telefónica, Telecom, Fibertel, Cablevisión, y CTI. Las mismas, utilizan los desarrollos de Cisco para satisfacer a sus clientes y fortalecer sus servicios. Comercial engloba a un espectro más amplio de empresas que incluye a las medianas y pequeñas; y por último aparece Home Networking, una opción que nace a partir de la compra de Linksys, una firma dedicada a la conectividad en el hogar. "De este modo, no sólo continuamenos conectando a las empresas, sino que ahora también a las personas y los hogares; la idea es llevar la tecnología de redes a la casa", desarrolla Ballerini, indicando que el enfoque planteado en cada uno de los cuatro modelos tiene su propia perspectiva en lo que se refiere al desarrollo de los productos y al público que los aplica en su vida.

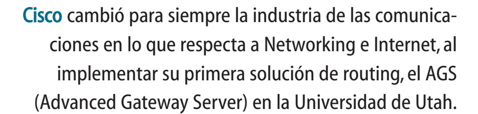
Mientras que, observando las propuestas tecnológicas de la familia Cisco, destacan:

- Routing y Swhiching: Clasificado como el centro de la empresa, y representando, en Argentina, alrededor del 80% del negocio.
- Tecnologías Avanzadas: Este modelo comprende varias de las principales innovaciones de estos últimos tiempos. De esta forma, está presente la Telefonía IP, que Cisco Argentina ve con mucho entusiasmo, teniendo en cuenta que el año pasado duplicaron las ventas en relación con las PBX tradicionales. Cabe destacar el acuerdo logrado con el Instituto Tecnológico de Estudios Superiores Monterrey, México, mediante el cual Cisco llevará a cabo investigaciones en conjunto con la entidad académica, además de proveerle 17 mil teléfonos IP de tal manera que sean reemplazadas las comunicaciones tradicionales, siendo ésta la más grande implementación de Telefonía IP de Latinoamérica. También, la Seguridad es un terreno que aparece en la lista, "porque la complejidad de las redes y la necesidad de proteger la información de las compañías hace que la inversión en seguridad esté al tope de la agenda de cualquier empresa". Por último, están las tecnologías Wireless, donde destaca la presencia de los proveedores de ISP como clientes (Arnet, Speedy, y más), y paralelamente con el auge de la conectividad inalámbrica, están las soluciones de Storage, que facilitan el acceso a la información y se presentan como la "posibilidad de la virtualidad de la información", y en ese sentido, "las redes cumplen un papel clave facilitando el acceso a los datos almacenados".
Cisco mantiene un fuerte lazo con los entornos educativos, de hecho en el directorio de la empresa debe haber un miembro de la Universidad de Stanford, entidad con la que lleva una relación directa sin olvidar de que fue allí donde todo comenzó. Del total de la facturación, Cisco destina US$ 3.2 mil millones en Investigación y Desarrollo, lo cual supone ser más del 15%. En el mundo, describe Ballerini, "tenemos mil laboratorios, e independientemente de las distancias y la cantidad de personas involucradas, se trabaja de manera conjunta". De aquellos mil centros de investigación, 500 están ubicados en San José, California, mientras que la otra mitad está en distintos puntos fuera de norteamérica; es el caso de India, Europa, e Israel entre otros lugares de prestigio para Cisco. "En Argentina tenemos una participación, desde el punto de vista de la investigación, orientada a la inversión de mercado. Sí, tenemos a veces convenios con universidades, para soportar ciertos temas particulares, pero no específicamente el desarrollo de tecnología. En general, estamos enfocados a los comportamientos de mercado, relacionado con el posicionamiento de nuestras soluciones".



Sebastián Ballerini
Gerente General de Cisco Systems para Argentina





Cisco cambió para siempre la industria de las comunicaciones en lo que respecta a Networking e Internet, al implementar su primera solución de routing, el AGS (Advanced Gateway Server) en la Universidad de Utah.

También, en el marco educativo destaca el Programa Cisco Networking Academy, que está conformada por más de 10 mil centros (más de 700 en América Latina), distribuidos en 152 países. Se trata de una forma directa a través de la cual proveer a estudiantes con las últimas herramientas en redes informáticas.
Ballerini cuenta, "somos empresa con raíces universitarias, de modo tal que la educación está en un lugar bastante alto en la agenda de Cisco. Siempre que podemos colaborar, lo hacemos. En Argentina acostumbramos llevar productos de networking para aportar tecnología y compartir visiones, además de informar sobre los desarrollos en los que trabajamos. Es, por ejemplo, la situación que se da en algunas de las carreras de postgrado de la Escuela de Dirección y Negocios de la Universidad Austral, donde nosotros presentamos el caso Cisco: Tecnología de la Información aplicada al Negocio".

Hacia el diseño de redes que piensan

Los desarrollos de Cisco influyeron sobre la construcción de la red, y los modos en los que se la utiliza, tanto a nivel corporativo como hogareño. Porque precisamente es allí donde rigen las bases de las principales soluciones de Cisco. Internet, con quince años más que Cisco, ha visto el crecimiento de la empresa en paralelo con el propio.
Ballerini describe un innovador concepto, donde la seguridad y el dinamismo convergen en el uso de redes informáticas dentro de entornos corporativos. Self-Defending Network es el nombre asignado a esta propuesta, que se desenvelve bajo el concepto de "empezar a integrar la seguridad en el nivel de las redes, para que éstas tengan mecanismos que les permitan reaccionar frente a parámetros no tradicionales de tráfico, dando como resultado acciones preventivas y no correctivas. Eso significa que si aparece un nuevo virus, la red será capaz de comprender el comportamiento anómalo y de esta manera lo aislará".
Un posible escenario, es cuando un usuario de la red decide conectarse utilizando una red pública en lugar de la propia conexión segura, con lo cual es posible que ingresen aplicaciones maliciosas, como por ejemplo un troyano. Entonces, cuando este usuario vuleva a formar parte de la red privada, ésta llevará a cabo procesos de comprobación del sistema antes de permitirle el acceso, para prevenir posibles infecciones. Incluso, la red tiene la habilidad de detectar la ausencia de parches, y en tal caso, instalarlos.
Y como no podía ser de otra manera, hablamos acerca de la evolución de las redes. Ballerini responde que desde Cisco "creemos que hay tres fases, conformadas por el transporte integrado (la convergencia de redes, como puede ser de voz y datos); servicios integrados (que pueden verse como una especie de service exchange framework, del cual un servicio puede estar disponible para cualquier miembro de la red, independientemente del medio de acceso); y la tercera fase, simplificaciones integradas". Esta última fase consiste en compartir los recursos de la red, de manera tal que no haya un solo procesador central encargado de ejecutar todas las tareas. Con el título de Intelligent Information Network, este modelo hace posible que "la red comience a entender qué aplicaciones tiene uno, para administrar la calidad del servicio y reconfigurar los sietmas en función de los distintos accesos y la información que es transferida".
Se trata de un mundo donde la computación trata de pensar sus acciones, en beneficio de un aumento en la productividad y en la accesibilidad diaria. Un mundo que aguarda del otro lado del puente.

simple
poweredbycisco.

Adquiera los nuevos routers de Cisco con servicios integrados de seguridad, movilidad y voz en un solo producto. Cisco ofrece soluciones para que las empresas de cualquier tamaño puedan reducir sus costos, simplificar los procesos y facilitar la administración de las redes. Los nuevos routers de Cisco administran fácilmente redes privadas virtuales -VPN, ofrecen funciones de firewall, QoS, enrutamiento de datos y conexiones inalámbricas de alta velocidad. Ingrese a **www.cisco.com/offer/isrnexit** o comuníquese al **0810-444-CISCO (24726)** y descubra la tecnología avanzada de los routers de servicios integrados de Cisco.

©2005 Cisco Systems, Inc. Todos los derechos reservados.



Cisco Systems

innovation. powered by



El Programa y su contribución a la formación de recursos humanos.

Cisco Networking Academy es un programa educativo sistemático, creado por Cisco Systems, que enseña a los estudiantes habilidades tecnológicas de Internet, utilizando una avanzada infraestructura de e-learning de alcance global. Desarrollado por educadores y expertos en diferentes áreas tecnológicas, el Programa proporciona contenidos basados en la Web, pruebas en línea, seguimiento y evaluación del desempeño de los estudiantes, prácticas de laboratorio, soporte y entrenamiento por parte de instructores calificados y preparación para acceder a certificaciones reconocidas por la industria.

El origen

El Programa tuvo su origen en un proyecto para el ámbito educativo en los Estados Unidos, en esa oportunidad Cisco realizó un acuerdo con educadores para generar oportunidades de crecimiento a partir de los desafíos que planteaba la tecnología y a su vez, diseñar redes prácticas y de bajo costo para las escuelas. Poco después, la compañía comenzó a desarrollar programas de capacitación para los educadores. Esto inspiró la creación de un programa de seminarios para desarrollar en todo Estados Unidos, cuyo éxito motivó el diseño de un plan de estudios para integrarlo como programa optativo. La respuesta fue el Cisco Networking Academy Program.

La primera versión del Programa fue lanzada en los Estados Unidos en octubre de 1997, en 64 instituciones educativas de siete estados. Desde entonces y gracias a su éxito, el Programa ha ido evolucionando en contenidos, infraestructura tecnológica, ámbitos de aplicación y otros aspectos, que han permitido que hoy Cisco Networking Academy esté presente en más de 150 países y cuente con más de 500.000 estudiantes activos inscriptos en más de 11.000 Academias en todo el mundo. Internet permite que los alumnos accedan a los contenidos en cualquier lugar a cualquier hora, independientemente de su ubicación, situación socioeconómica, sexo o raza.

Hoy el Programa está presente en más de 150 países y cuenta con más de 500.000 estudiantes activos inscriptos en más de 11.000 Academias en todo el mundo.

Las Academias y la currícula

Para llevar adelante la administración y operación del Programa se identifican tres niveles organizativos: los CATC (Cisco Academy Training Centers) que capacitan a las Academias Regionales que tienen asignadas, éstas a su vez capacitan a las Academias Locales que dependen de ellas. Las Academias Locales por su parte tienen la misión de capacitar a los estudiantes. En todos los casos, la capacitación está a cargo de instructores certificados en la especialidad que corresponda a la carrera que dicten y que deben re-certificarse periódicamente para poder tener una clase a su cargo.

Inicialmente creado para preparar estudiantes para los niveles CCNA (Cisco Certified Network Associate) y CCNP (Cisco Certified Network Professional), la oferta educativa del Programa se ha extendido gracias a los programas de capacitación patrocinados por los socios del ecosistema, entre los que se incluyen: Fundamentos de Tecnologías de la Información, patrocinados por Hewlett-Packard; Fundamentos de Interconexión de Redes, patrocinado por Panduit y Fundamentos de Unix y Java.

El núcleo principal de la currícula lo constituyen los programas denominados CCNA y CCNP. El primero consta a su vez de cuatro módulos que proporcionan formación sobre Networking, Routing, Switching y tecnologías WAN. El segundo, por su parte, provee formación en Routing avanzado, Acceso remoto, Switching Multicapa y Solución de Problemas en Redes. La formación adquirida capacita a los estudiantes para rendir los exámenes requeridos para obtener certificaciones reconocidas por la industria a nivel internacional.

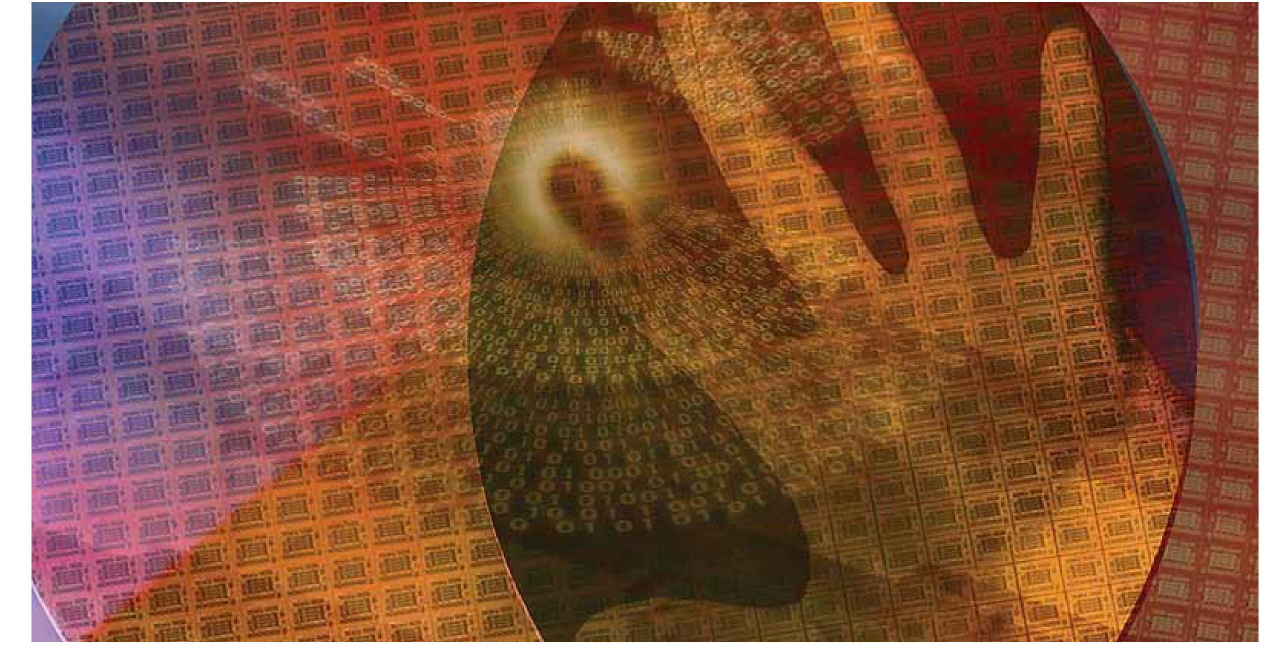
La currícula incluye además otros programas de formación tales como Fundamentos de Wireless LAN y Fundamentos de Seguridad en Redes. Actualmente, Cisco Networking Academy está trabajando en una nueva oferta educativa sobre Telefonía IP, orientada a ser integrada en los programas regulares de nivel universitario.

Es oportuno destacar que para complementar la capacitación inicial ofrecida por Cisco Networking Academy Program, la compañía cuenta también con una estructura formal de capacitación, entrenamiento y certificación profesional por medio de sus Learning Partners como agentes capacitados y autorizados para estos servicios.

Responsabilidad Social

El origen y la naturaleza del Programa Cisco Networking Academy son elementos clave para entender porqué el mismo es parte de los proyectos de responsabilidad social de Cisco Systems. El Programa está orientado hacia la sociedad, particularmente hacia los ámbitos académicos de nivel universitario, terciario, institutos y organizaciones educativas de nivel técnico. La compañía desarrolla los contenidos y proporciona la plataforma de e-learning y soporte comunicacional para la comunidad

FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

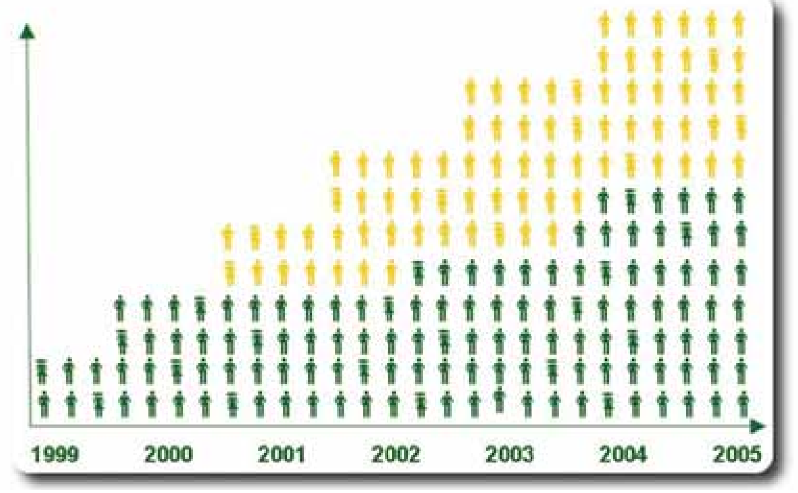


mundial del Cisco Networking Academy en forma gratuita para las Academias.
Los cursos que integran la curricula permiten complementar la enseñanza que se brinda según la estructura formal de las casas de estudio, mediante el aporte de conocimientos y práctica sobre equipos que permiten emular muchas de las condiciones que se presentan en las instalaciones en el mundo real de las empresas u otras organizaciones. Esto representa un valor agregado de importancia para los estudiantes, que de esta forma tienen mayores oportunidades de integrarse al mundo tecnológico y globalizado actual y tener mayores oportunidades al momento de competir en el mercado laboral.
Asimismo y consecuentemente con la visión de Cisco Systems, el Programa se desarrolla en un ecosistema integrado por ámbitos educativos, gobiernos y entidades que, concientes de la importancia de educación en tecnología, dan soporte al Programa y empresas líderes que bajo acuerdo con Cisco Systems aportan contenido que contribuye a formar un cuerpo consistente y completo de conocimientos teórico-prácticos. Este ecosistema permite entonces ofrecer todo el rango de servicios y soporte necesario para el crecimiento de la fuerza laboral del mañana. Así lo confirma John Chambers, CEO de Cisco Systems,: "Los trabajos del futuro irán donde se encuentre la fuerza laboral mejor educada, la infraestructura correcta y el apoyo adecuado por parte del Gobierno".

El Programa en Latinoamérica

Latinoamérica no ha estado ausente al momento de sumarse al proyecto y hoy se pueden dar algunas cifras que hablan por sí mismas. El programa cuenta regionalmente con 730 Academias que incluyen CATCs, Academias Regionales y Academias Locales, distribuidas en 24 países. El total de estudiantes activos suma casi 72.000 y el de Instructores alrededor de 2.700.
Por otra parte, y como punto de integración entre todos los estudiantes de la Región, desde mayo de 2004 comenzó a funcionar Academy Connection en español, un portal que busca impulsar la interacción entre los usuarios de 21 países de habla hispana donde el programa tiene presencia. Para ello, cuenta con un equipo de corresponsales que aporta noticias, estadísticas, publicaciones en los medios, testimonios, proyectos y contactos.
Concentrando la atención en la región que comprende a Argentina, Bolivia, Paraguay y Uruguay, se puede hacer foco en el éxito particular que ha tenido el desarrollo del Programa desde sus inicios, a partir del año 1998, cuando se suscribe el acuerdo entre Cisco y la Fundación Proydesa, que es designada como Academia Regional a partir de entonces.
Desde el comienzo, el trabajo de adaptación a las características de la Región dio como resultado una creciente convocatoria para CCNA, que hoy cuenta con más de 16.000 integrantes.
La estructura del Programa en la Región tiene a Fundación Proydesa como Academia Regional, que a su vez funciona como Regional Server con soporte para todo lo concerniente a contenidos, herramientas, presentaciones y recursos de alumnos. Además, desde 2001 fue designada como Academia CCNP (Cisco Certified Network Professional) y se constituyó en el primer Cisco Academy Training Center (CATC) con capacidad para capacitar a Academias Regionales.
Como Academia Regional, Proydesa ha

"Los trabajos del futuro irán donde se encuentre la fuerza laboral mejor educada, la infraestructura correcta y el apoyo adecuado por parte del Gobierno". John Chambers, CEO de Cisco Systems



Evolución de alumnos y egresados por año.

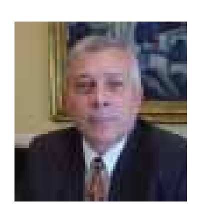
contribuido a desplegar 53 Academias Locales, que cuentan con casi 200 instructores, que a su vez enseñan a unos 6.300 estudiantes activos. A esto debemos agregar los casi 10.000 egresados que se han formado con el Programa. La clave de la aceptación del Programa en la región ha sido, no solo el reconocimiento de la importancia y calidad del Programa, sino también la profesionalidad con que se ha llevado a cabo su despliegue y posterior operación en la región.

Cisco Networking Academy, con sus Academias Locales ubicadas en puntos estratégicos de la Región, ha sabido dar respuesta a necesidades específicas de conocimiento que impone el mundo globalizado actual, ampliando la oferta de carreras tecnológicas, haciéndolas accesibles a todas las capas de la población sin resignar nada en cuanto a calidad pedagógica. De esta manera Cisco Systems contribuye como parte de sus objetivos de responsabilidad social, con los objetivos de desarrollo de la sociedad en la que actúa, a través de la educación y formación de recursos humanos en tecnología de la información. ■

La capacitación está a cargo de instructores certificados por Cisco Systems. Estos instructores deben re-certificarse periódicamente para poder tener una clase a su cargo.



Jorge Hedderwick
Área Academy Manager Cisco Networking Academy Cisco Systems



César Barbaglia
Main Contact Fundación Proydesa CATC & Regional Academy

Web Site de Pasantías y Laboral: Nexo entre los recursos humanos calificados y el mundo empresario

En respuesta a la necesidad de buscar una forma eficaz de vincular a las empresas usuarias de tecnología con los recursos humanos altamente calificados en toda la región, en el año 2000 Fundación Proydesa gestó un proyecto que derivó en el actual Web Site de Pasantías y Laboral.

El Web Site de Pasantías y Laboral (http://rrhh.proydesa.org) es un servicio que vincula a la comunidad de alumnos y egresados de Cisco Networking Academy en la región con aquellas empresas que los necesitan, contribuyendo de esta manera a cerrar el círculo de la producción y la capacitación.

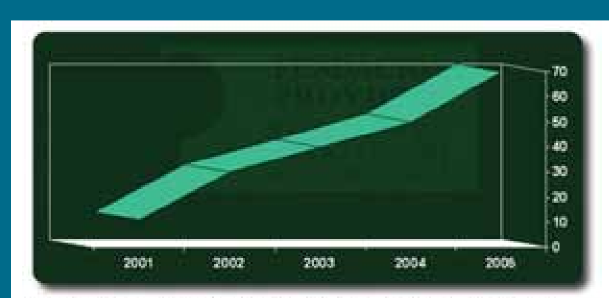
La particularidad de este Web Site de Pasantías y Laboral, es que se ha convertido en un canal directo que armoniza los intereses de empresas y alumnos. Toda Organización inscripta puede publicar su oferta laboral o elegir entre los más de 4.000 curriculum vitae de estudiantes validados por Instructores certificados por Cisco Systems, y contactarlos bajo estrictas normas de confidencialidad.

Si el mundo empresarial no advierte a tiempo que el personal de la empresa es su activo más valioso, en un futuro próximo estará lamentando las consecuencias.

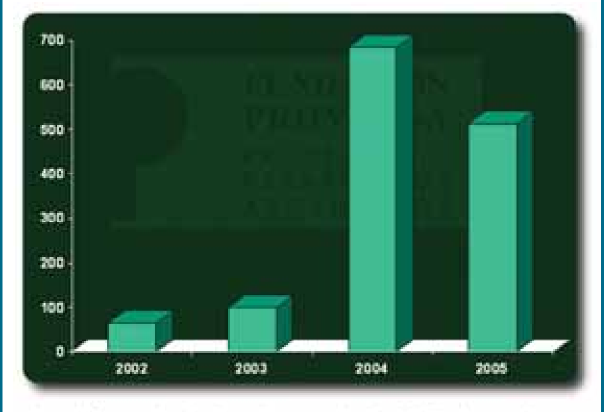
El cumplimiento de los objetivos del proyecto es satisfactorio, teniendo en cuenta algunos indicadores. Desde su implementación, se ha incrementado en forma continua la cantidad de empresas que utilizan el servicio, llegando a la fecha a integrarlo 70 organizaciones de primera línea, entre las que se cuentan Cisco Systems, Oracle, IBM, HP, iPlan Networks, Telefónica, Telecom, Software del Plata, entre otras.

La participación de las empresas ha dado como resultado un incremento en las publicaciones de ofertas laborales. Así, en el año 2004, y luego de una recuperación que ya venía anunciándose en la segunda mitad del año anterior, las empresas publicaron ofertas laborales que superaron en un 600% las publicadas en el año anterior. El año 2005 mantiene hasta ahora la misma tendencia.

En resumen, el Web Site de Pasantías y Laboral ha demostrado ser una herramienta eficaz, y forma parte de la concepción de Cisco Networking Academy y de los objetivos fundacionales de Fundación Proydesa como un aporte al tejido social de nuestro país.



La utilización del servicio ha experimentado un marcado crecimiento por parte de las empresas demandantes.



Las búsquedas laborales en el año 2005 siguen la misma tendencia de crecimiento que en el año anterior.

Llegaron los sapos!!!

Si no quiere tragarse uno,
antes de elegir a su proveedor de tecnología considere:

Expertise
Experiencia

- Cisco Systems IP Communications Specialization
- Cisco Systems Security VPN/Firewall E. Specialization
- Tyco AMP Gold NDI Partner Contractor
- APC Corporate Partner
- 12 Años certificando calidad

Telefonía IP, VoIP, VPN Security, Fiber & Cable, Wireless LAN, Routing & Switching, Management.

Concepción Arenal 2978 · C1426DGH · Bs. As. · Argentina · Tel.: (5411) 4777-7564 · Fax : 4773-0547





Cisco Internetwork Operating System (IOS)

Cisco IOS (originalmente entendido como Internetwork Operating System) es el sistema operativo usado en los routers y switches de CISCO Systems (algunos de sus switches todavía cuentan también con el sistema operativo CatOS). Es un sistema operativo multitasking y provee servicios de kernel tales como scheduling de procesos como también la interfase de línea de comandos (command line interface) y software de routing.

Cisco IOS tiene una interfase de línea de comandos muy característico, cuyo estilo ha sido copiado por otros softwares de networking. A diferencia de la mayoría de los sistemas operativos que usan un comando seguido por un conjunto de "argumentos", el IOS de Cisco provee un conjunto fijo de comandos con múltiples palabras. El conjunto de comandos disponibles está determinado por el "mode" (modo), por ejemplo, el "global configuration mode" (modo de configuración múltiple), nos provee comandos para cambiar la configuración del sistema y el "interface configuration mode" provee comandos para cambiar la configuración de una interfase específica de capa 2 (layer 2). Un comando típico puede ser:"show interface gi0/48" or "no ip cef traffic-statistics". A todos los comandos se les asigna un "privilege level" (nivel de privilegio), que va de 0 a 15, y puede ser solo accedido por usuarios con los privilegios necesarios.

Versiónes del CISCO IOS.

Las versiones del Cisco IOS están caracterizadas por tres números y algunas letras, en un formato x. y(z)aa, donde

- x es el "major version number" del release
- y es el "minor version number"
- z es el número del release, que comienza en 1 y se incrementa cuando aparecen nuevos maintenance releases en el mismo "x.y train"
- a es el identificador de "release train", tal como nada (que identifica la línea principal (mainline), T(para tecnología), E (para Enterprise), S (para Service provider), etc.

Por ejemplo, el release 12.3 (1) es el primer mainline release de CISCO IOS de la versión 12.3 12.3 (2) es el release que le sigue, y así siguiendo. 12.3 (1) T es el primer release del T train, 12.3 (2) T el que le sigue.

Los trains de CISCO IOS

Los release de Cisco IOS están divididos en varios "trains", cada uno con características diferentes. Los "trains" se mapean aproximadamente a distintos mercados o grupos de clientes. El llamado "mainline release" está diseñado para ser el release más estable que la empresa puede ofrecer y su "feature set" nunca se incrementa durante su vida. (solo se mejoran con correcciones a bugs). El "train" T (tecnología) podrá incorporar nuevas características y soluciones a bugs durante su vida, y por tanto es menos estable que el "mainline". El "train" S (Service provider) corre solamente en los productos especializados para los clientes Service Providers (carrier/PPT) El "train" E está customizado para routers del segmento Enterprise. Aparecen cada tanto otros "trains", que se los designa para necesidades específicas. Por ejemplo, el "train" 12.0AA contenía nuevo código requerido para la línea de productos CISCO 5800.

"Feature sets" de CISCO IOS

Cada release tiene uno o más "feature sets", por ejemplo, las versiones de IOS diseñadas para los switches Catalyst están disponibles como versiones"standard" (que proveen solo un routing IP básico), "enhanced", que provee soporte de routing IPv4 full y versión "advanced IP services", que provee las características de "enhanced" con soporte para IPv6.

La arquitectura de CISCO IOS.

En todas las versiones del Cisco IOS, packet routing y forwarding (switching) son funciones diferentes. Routing y otros protocolos corren como procesos del Cisco IOS y finalmente resultan en una tabla de forwarding (la FIB, Forwarding Information Base), que es usada por la función forwarding del router. En plataformas de router con software "solo forwarding" (por ejemplo Cisco 7200) el manejo del tráfico, incluyendo listas de control de acceso (Acccess control lists) para filtrado y forwarding que se realiza al nivel de interrupción (interrupt level) usando el "Cisco Express Forwarding (CEF) o dCEF (Distributed CEF).

Esto significa que IOS no tiene que realizar un "process context" para forwardear un paquete. En routers con forwarding hardware-based (basado en hardware) tal como la serie Cisco 12000, el Cisco IOS computa la FIB en software y la carga en el hardware de forwarding (tal como un ASIC o "network processor"), que realiza la función de forwardear el paquete.

El Cisco IOS, tiene una arquitectura "monolítica", que significa que corre como un imagen "single" y todos los procesos comparten el mismo espacio de memoria. No hay protección de memoria entre procesos. Tiene además un scheduller "run to completion", que significa que el kernel no hace un "pre empt." de un proceso que ya corre. El proceso debe hacer un llamado al kernel antes que otros procesos tengan chance de correr.

Para los productos Cisco que requieren gran disponibilidad, tal como el CISCO CRS-1, estas limitaciones no eran aceptables. La respuesta de CISCO fue la de desarrollar una nueva versión del Cisco IOS, llamada IOS-XR que ofrece modularidad y protección de memoria entre procesos, junto con threads livianos y scheduling "pre-emptive". Esta versionde IOS-XR tambien esta disponible para la linea de routers GSRs.

En agosto del 2005, Cisco anunció su nueva versión de IOS para sus switches de línea alta con un diseño modular. Dejando de lado el kernel monolítico de versiones anteriores, el nuevo IOS permitirá procesos "re-starteables" individualmente, que podrán ser parcheados independientemente de otros procesos y del IOS como un todo. Este diseño modular le permitirá al administrador patchear sólo procesos afectados. Luego del patching, ese proceso particular podrá ser "re-starteado" independientemente del resto del switch, reduciendo el "downtime" total al mínimo.

Fuente: www.wikipedia.org



Confíe sus comunicaciones de negocios a una sola red con Equant IP Telephony.

Las comunicaciones de negocios toman múltiples formas – desde documentos hasta decisiones, desde charlas a conferencias. Equant IP Telephony las combina todas en un solo lugar.

Ponga sus servicios de voz en una red de datos. La telefonía IP va más allá de la voz sobre IP – es una solución completa. Por ejemplo, puede añadir aplicaciones como mensajería unificada y podrá ver todas las llamadas e emails en un solo lugar. Esto es sólo el comienzo..., servicios de Callcenter centralizados y/o distribuidos...; siguiendo el sol...; el idioma...; o simplemente, siguiendo las necesidades.

Vea como sus costos bajan. Tarifas de larga distancia serán una cosa del pasado. Visite **www.equant.com** para ver como puede hacer que la Telefonía IP sea parte de su futuro.

Para mayor información puede contactarse con nosotros en nuestras oficinas de Buenos Aires, sitas en Ing. Butty 240, Piso 3° - Edificio Laminar o al teléfono (54 11) 4590-3700





Cisco Systems
Gold Certified Partner

inteligencia interior





Intel® Xeon™ de 64 bits y **Windows® Server 2003 x64** lograron mejorar la disponibilidad, confiabilidad, potencia, flexibilidad y performance de su tecnología en ambientes de misión crítica. Ahora la plataforma de servidores más ampliamente utilizada del mundo soporta aplicaciones de 64 bits. El procesador Intel® Xeon™ de 64 bits posee capacidades de ahorro de energía mejoradas, memoria flexible, mejoras en procesos de entrada/salida y almacenamiento configurable. Y, por supuesto, continúa soportando todas las aplicaciones de 32 bits. **Porque el poder está en el interior.**





Para más información contáctese con su proveedor de confianza.

www.intel.com/business

Multiprotocol Label Switching (MPLS)

MPLS (Multiprotocol Label Switching) es un mecanismo de "data-carrying" (acarreo de datos), que opera en una capa debajo de protocolos como IP. Fue diseñado para proveer un servicio de "data-carrying" unificado para clientes "circuit-based" y clientes "packet-switching" que brindan un modelo de servicio de datagrama. Puede ser utilizado para proveer diferentes tipos de tráfico, incluyendo tráfico de voz telefónica y paquetes IP.

Background

Un número de diferentes tecnologías fueron implementadas anteriormente con propósitos similares, tales como frame relay y ATM. MPLS está hoy reemplazando estas tecnologías.
En particular, MPLS abandona la idea de "cell-switching" y "signaling-protocol" de ATM. MPLS reconoce que las pequeñas celdas (cells) de ATM no son necesarias en networks modernos, ya que las redes ópticas modernas (desde 2001) son tan rápidas (10 GBits y más) que aún paquetes "full-length" de 1500 bytes no sufren retrasos (delays) de queuing (colas) significativos en tiempo real (la necesidad de reducir tales delays para soportar tráfico de voz ha sido la motivación de la naturaleza de celdas (cells) de ATM).
Al mismo tiempo, trata de preservar la ingeniería de tráfico y control "out-of band" que hizo a frame relay y ATM atractivos para implementar redes en gran escala.
MPLS fue originalmente propuesto por un grupo de ingenieros de Cisco Systems, Inc. Y fue llamado "Tag switching" cuando fue entregado al IETF para una estandarización abierta. Una de las motivaciones originales fue la de permitir la creación de switches de alta velocidad simples, ya que se pensó en determinado momento que sería imposible hacer un "forward" de paquetes IP en hardware.. Sin embargo los avances en VLSI (Very Large Scale Integration, Integración en gran escala) ha hecho posible la existencia de tales dispositivos

Como funciona MPLS

MPLS funciona adicionando a los paquetes un header MPLS, que contiene uno o más "labels" (etiquetas). Esto se llama un "label stack"
Cada entrada del "label stack" contiene cuatro campos (ver fig.1):
- un valor de 20bits llamado "label"
- un campo experimental de 3 bits reservado para futuro (Exp)
- un flag de 1 bit :"bottom of snack" (bit S)
- un campo TTL (time to live) de 8 bits.

Estos paquetes MPLS son forwardeados (switcheados sería el término correcto) luego de un Label Lookup/Switch en lugar de un lokup en la tabla IP. "Label Lookup" y "Label Switching" puede ser más rápido que un "RIB lookup" usual ya que puede hacerse en fabric y no en CPU.
En fin, mas allá de las motivaciones originales de crear switches mas rápidos, MPLS se convirtió en la tecnología que posibilita la entrega de diversos servicios necesarios en la redes de hoy, todos ellos sobre una misma red. Por tal motivo es la tecnología elegida para realizar la convergencia de redes. Algunos de estos servicios son:
- IP
- QoS (Quality of Services)
- VPNs (Virtual Private Networks)
- TE (Traffic Engineering)
- IP+Optical GMPLS
- AToM (Any Transport over MPLS) para servicios de nivel dos como:
    - ATM
    - Frame Relay
    - HDLC
    - PPP
    - Ethernet

MPLS y Cisco

El MPLS del Cisco IOS junta la inteligencia del routing con la performance del switching y da beneficios importantes tanto a redes con una arquitectura IP pura, como también a aquellas con IP y ATM o mezcla de otras tecnologías de capa 2 (Layer 2). La tecnología MPLS es clave para la escalabilidad de VPNs (Virtual Private Networks) y QoS (Quality of Service, calidad de servicio) end-to-end. Permite la utilización eficiente de las redes actuales para enfrentar crecimientos futuros y corrección rápida de fallas en links y nodos. La tecnología permite además poder implementar servicios IP diferenciados end-to-end, altamente escalables, con configuraciones, administración e implementaciones simples tanto para proveedores de Internet y suscriptores.

Fuente: www.wikipedia.org

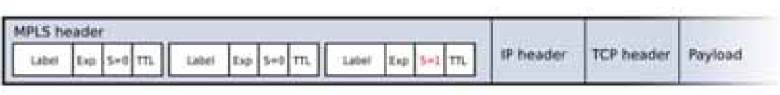
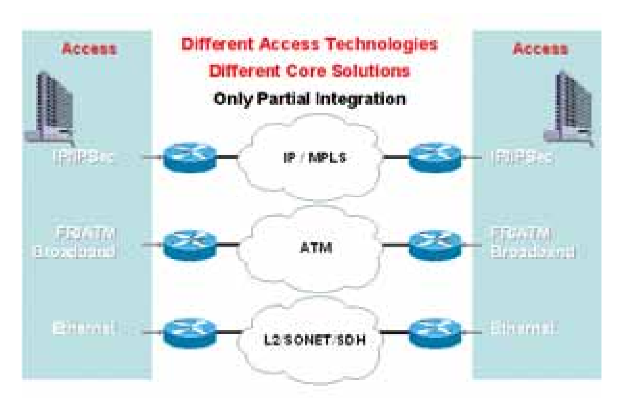
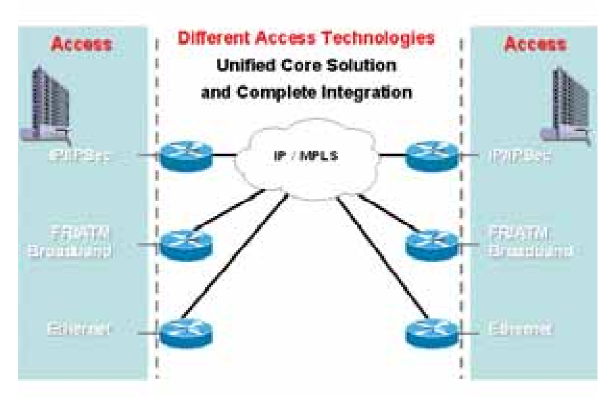


Figura 1. "Label Stack"



Esquema de distintas redes tradicionales



Esquema de Convergencia de redes con MPLS



Autor: **Steve Hratko**
Traducción: **Leonel Becchio**

Convergencia móvil-fija

Uniendo tecnologías de acceso LAN y WAN inalámbricas para obtener un servicio homogéneo.

Es una creencia ampliamente sostenida que la mayoría de los accesos a la red serán eventualmente libres de ataduras. Las PDA´s, teléfonos celulares, laptops y dispositivos basados en IP harán uso de la tecnología de radio para conectarse a la red. La mejor solución provendrá de una combinación de tecnologías de radio de LAN inalámbricas basadas en el estándar IEEE 802.11 para lograr una alta performance en lo que a área local se refiere –tales como hoteles, aeronáutica o edificios de oficinas– y de un servicio móvil de radio para accesos ubicuos (WAN inalámbrica). Esta unión homogénea de servicios de telefonía móvil y de accesos de banda ancha y LAN inalámbrica se denomina convergencia móvil-fija.

Las opciones móviles de radio incluyen CDMA2000 y su capa de datos de alta velocidad EV-DO (evolución – datos optimizados), y GSM/UMTS con su capa de alta velocidad HSDPA (acceso de descarga de paquetes de alta velocidad). Agregado a estas opciones, existen dos nuevas tecnologías móviles provenientes de IEEE que pronto formarán su camino hacia el mercado. Son conocidas como 802.20 y 802.16 (WiMAX).

Hay una cantidad de otras tecnologías móviles de datos puestas en uso, que incluyen GPRS, EDGE, CDMA 1x y UMTS las cuales transportan voz y datos en la misma portadora de radiofrecuencia; sin embargo, no es la solución más ventajosa en términos de eficiencia espectral a causa de que los requerimientos de voz son muy diferentes a los de datos. Las nuevas opciones de radio de alta performance colocan la voz en una portadora y los datos en otra.

Los beneficios de esta convergencia de servicios móviles-fijos para usuarios finales son una mejor conectividad siempre utilizando la señal de radio que se encuentre más disponible en ese momento y en ese lugar. Este acercamiento es beneficioso cuando se utiliza telefonía móvil en edificios, ya que es allí donde la tecnología Wi-Fi se utiliza en mayor medida y donde las señales móviles pueden ser más débiles.

Uno de los beneficios de esta convergencia para operadores móviles es que les permite transportar un montón de comunicaciones que a menudo van hacia los operadores telefónicos, con lo cual acelera la sustitución de la convergencia móvil-fija. También provee una muy buena respuesta a los proveedores de voz sobre banda ancha que están saliendo a la luz en todas las geografías. Estos proveedores utilizan voz sobre IP (VoIP) sobre banda ancha para encauzar las comunicaciones y lo hacen a un precio mucho más bajo que los operadores tradicionales.

El teléfono de doble-modo es una gran respuesta a esta amenaza ya que provee voz sobre banda ancha con movilidad completa. El trasfondo para los operadores reside en una experiencia de usuario mucho mejor, hecho que mejoraría su posición competitiva.

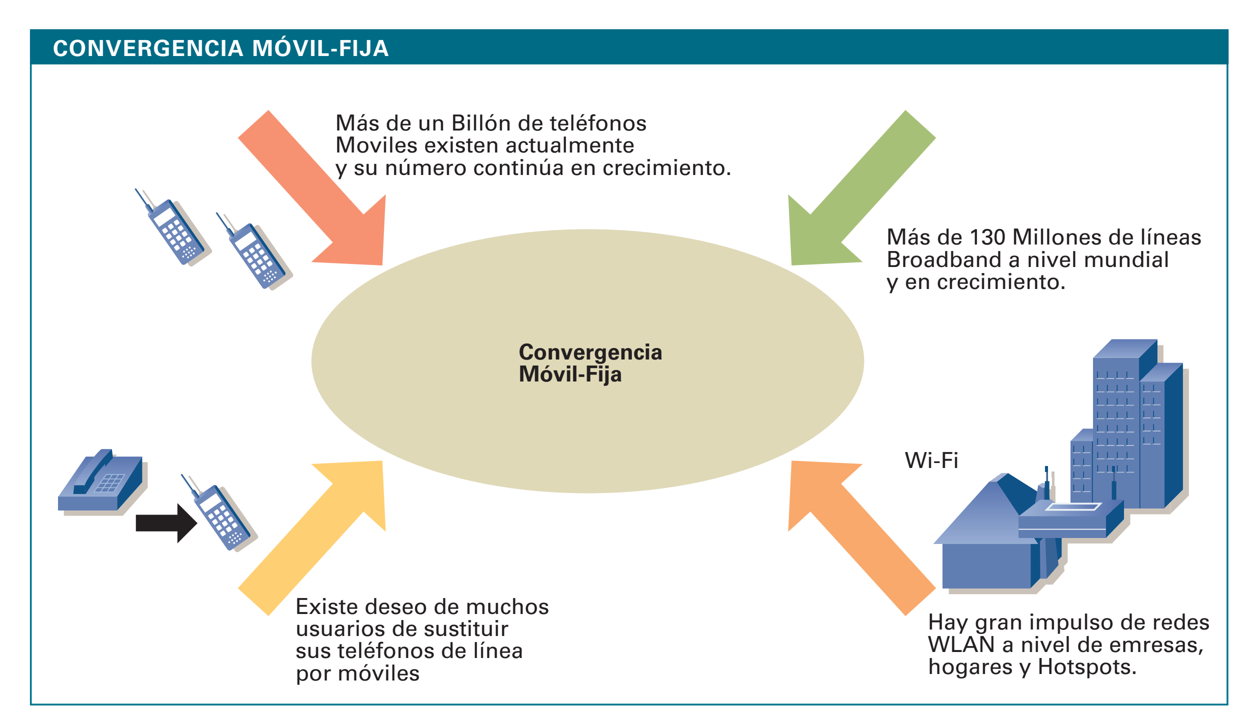
Uniendo diferentes tecnologías de acceso de radio

Los operadores móviles usarán una variedad de propuestas para permitir que las diferentes tecnologías de acceso por radio permitan repartir una oferta de servicios convergentes. Estos incluyen:

• Acceso móvil no licenciado (UMA, Unlicenced Mobil Access) es una nueva tecnología de capa 2 idealmente adaptada para ofrecer servicios de voz utilizando el centro de conmutación de operadores móviles para llamadas de control sobre accesos GSM o IP de banda ancha. Con una red IP de banda ancha, la señalización de voz GSM y portadora son tunelizadas a través de la red IP y vuelve al dominio del operador móvil. Mientras el usuario se mueve entre Wi-Fi y la cobertura GSM, la red manipulará la llamada. Con una red diseñada en forma conveniente, el usuario no experimenta degradación alguna del servicio. Esta tecnología es especialmente adaptada en lugares donde la cobertura celular requiere se suplementada con cobertura Wi-Fi, y podría comenzar a emerger en los próximos 12 a 18 meses.

• IP Móvil (Mobile IP)es una tecnología de capa 3 adaptada a servicios de datos basados en laptops (no requiere control de llamada de voz). Operadores tales como Swisscom Mobile (swisscom-mobile.ch) ya están ofreciendo servicios que utilizan las tarjetas PCMCIA trimodo que soportan Wi-Fi, GPRS o UMTS para

FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved



UNA TORMENTA EN EL MUNDO DE LAS TELE-COMUNICACIONES
Varios factores se juntan en el mudo del Broadband y la movilidad, de modo de potenciar la convergencia móvil-fija.

adquirir conectividad. La laptop selecciona la mejor señal de radio e IP Móvil permite gestionar mientras el usuario se mueve a través de diferentes áreas de cobertura. La fortaleza de IP Móvil es que permite a la laptop mantener su propia dirección IP mientras el usuario se moviliza. Esta tecnología ya está disponible y su implementación ya existe en varias partes del mundo.

• Protocolo de Inicio de Sesión (SIP, Session Initiation Protocol). La movilidad que brinda este protocolo de la capa de aplicación es el camino futuro para muchos de los proveedores de servicios. Éste permitirá soportar servicios multimedia en tiempo real. Una de las grandes ventajas de usar SIP en convergencia de servicios es que le permite al usuario transferir una sesión de aplicación entre dispositivos. Por ejemplo una sesión podría iniciarse en una laptop en la casa, pasarse a una PDA mientras el usuario ingresa en su auto y devolverse a la laptop cuando el usuario llegue a la oficina. Los requerimientos de SIP para multimedia en tiempo real basada en IP necesitan una inversión sustancial en las redes cableadas públicas y probablemente se extenderá por muchos años.

Hacer una combinación de diferentes tecnologías de acceso por radio es técnicamente desafiante y por eso vale la pena echarle un vistazo.

LAN inalámbricas

La tecnología dominante para redes LAN inalámbricas está basada en el estándar IEEE 802.11. Esta tecnología está ampliamente utilizada, es de costo efectivo, rápida y utiliza espectro no licenciado. Esto último tiene implicancias significativas de como puede implementarse esta tecnología, y no licenciado no significa no regulado. El uso de bandas no licenciadas pone limitaciones en la cantidad de potencia que un dispositivo 802.11 puede emitir. Una potencia de salida mayor causará interferencia con otros usuarios de esa banda.

Como tal, esta tecnología está siendo usada como soporte de servicios de LAN inalámbrica. Estos servicios pueden implicar un único punto de acceso en un café o una gran cantidad de puntos de acceso para cubrir un aeropuerto o una zona en un área suburbana.

Las redes inalámbricas típicamente tendrán una ventaja sobre los servicios móviles. La razón para esto incluye la simple física de las ondas de radio. La potencia de la señal de radio disminuye con el cuadrado de la distancia (y aun más rápido en algunas instancias). Por lo tanto, los usuarios más cercanos al punto de acceso, gozan de una señal más intensa y de una performance más elevada. Las LANs inalámbricas son usualmente encontradas en áreas de tráfico intenso (hoteles, aeropuertos y centros de convenciones) y solamente necesitan propagar una señal unos pocos cientos de metros. Un servicio móvil inalámbrico debe poder propagar señales decenas de kilómetros.

Otra ventaja que tienen las LANs inalámbricas sobre los servicios móviles es el ancho del canal de la portadora. Las LAN inalámbricas operan en bandas de frecuencias más altas y poseen canales más anchos. Los sistemas de hoy en día utilizan canales de 20 MHz y probablemente en el futuro incluirán opciones de canales más anchos y más estrechos. Los canales más anchos soportan velocidades de tráfico más elevadas. Mientras las bandas de alta frecuencia no penetran estructuras tanto como sí lo hacen las bandas celulares, esto puede ser una ventaja cuando se utilizan frecuencias no licenciadas ya que ayuda a limitar la interferencia.

WAN inalámbricas

Contrariamente, los sistemas de redes WAN inalámbricas operan en bandas de frecuencias más bajas y con canales más estrechos. Los canales más estrechos implican velocidades más bajas debido primariamente a la economía del espectro de radiofrecuencia. Espectros de frecuencias más bajos son más valiosos que las altas frecuencias y es traducido en anchos de banda más angostos.

Para aplicaciones móviles, las frecuencias óptimas se encuentran por debajo de 1 GHz. De hecho, en varias partes del mundo tuvieron éxito con servicios móviles que operaban a 450 MHz donde una torre celular podía cubrir la misma área que más de una docena de torres operando a 1,9 GHz (hay mucha variación acá dependiendo del terreno). Además en rangos de propagación más grandes, las frecuencias más bajas pueden también atravesar estructuras en forma más eficiente para llegar a los usuarios dentro de los edificios. Esto es muy importante para operadores y suscriptores quienes quieren conectividad ubicua.

Los operadores de redes inalámbricas móviles encaran una decisión desafiante respecto de cómo evolucionan sus redes para soportar servicios de datos de alta velocidad. Se anticipa que estas redes orientadas a datos serán implementadas como redes de capa usando espectros de RF dedicados. Ejemplo, usando portadoras de RF dedicadas a HSDPA, EV-DO o IEEE 802.16. Si los datos de alta velocidad fueran hechos para compartir el espectro de RF con la voz, esto podría degradar la habilidad del espectro cuando se necesite soportar tráfico de voz crítico.

Todas las tecnologías inalámbricas móviles orientadas a datos (HSDPA, EV-DO, 802.20 y 802.16) ofrecerán una performance similar. Como regla general, los usuarios pueden esperar alrededor de 500 a 600 Kbit/seg en el enlace descendente y 100 a 200 Kbit/seg en el ascendente. Las cifras variarán ampliamente dependiendo de variables tales como la distancia a la torre celular, la carga de la torre, el terreno, y el movimiento y la velocidad del usuario. Estas velocidades son solamente aproximaciones que mejorarán a medida que evolucione la tecnología.

Una mirada más cercana a 802.16 para tecnologías inalámbricas móviles

De todas las tecnologías inalámbricas móviles, IEEE 802.16 (también conocida como WiMAX) ha conseguido llamar la atención, debido al marketing exitoso a cargo del Foro WiMAX, un fuerte apoyo de vendors tales como Intel y la participación de los mayores vendors de servicios de acceso a la red por radio. WiMAX surgió como una tecnología inalámbrica fija que podía ser utilizada en aplicaciones de transporte de microondas así como para acceso inalámbrico fijo. Recientemente WiMAX ha comenzado a incor-

porar soporte para brindar movilidad.
Las ventajas primarias de las soluciones basadas en WiMAX incluyen las siguientes:
• Derechos de propiedad intelectual racionales que vienen acompañados de una política de licencias justas y no discriminantes provenientes del IEEE.
• Una fuerte campaña de marketing a través del Foro WiMAX, dedicado a promover dicha tecnología.
• Soporte de Intel, el cual se traduce en dispositivos cliente móviles más económicos a medida que la tecnología WiMAX se integra en laptops y PDAs.
Se acentúa este punto ya que el costo del dispositivo cliente móvil es una parte considerable del costo del servicio que a menudo debe ser subsidiado por el mismo operador del servicio móvil.
La desventaja primaria de la tecnología WiMAX es que, al menos hasta el año 2006, probablemente no surjan implementaciones reales basadas en este estándar. Mientras tanto, ya están disponibles las soluciones basadas en EV-DO y HSDPA.
El mercado para WiMAX incluye los siguientes:
• Transporte de microondas. Gran parte del mercado WiMAX se centra en el transporte de voz el cual se realiza a altas frecuencias (mayores a 10 GHz) utilizando la línea de vista. Los vendors en este mercado han adoptado soluciones propietarias y un estándar reduciría los costos.
• Acceso inalámbrico fijo. Este mercado es pequeño y se centraliza en áreas donde predomina la falta de servicios de cable y DSL La tecnología inalámbrica fija sufrió problemas de competencia frente a las soluciones cableadas cuando éstas estaban disponibles. WiMAX es capaz de llevar la tecnología inalámbrica a laptops y PDAs haciéndolas portables. Los usuarios comienzan a disfrutar de servicios DSL inalámbricos que los siguen mientras se mueven. Pero esto suena ya a servicios móviles.
• Gran mercado móvil. Los gastos de los operadores móviles de todo el mundo superan los 80.000 millones de dólares anuales y el negocio de los dispositivos clientes es aún mayor. Si WiMAX puede exitosamente erguirse como capa de datos móviles de alta velocidad, ayudará a reducir el costo de la tecnología para todas las aplicaciones.
WiMAX no será un competidor viable de Wi-Fi en la LAN, sino que es una tecnología WAN y por lo tanto competirá con otras tecnologías de su misma especie.
La convergencia móvil-fija será una de las tendencias dominantes de los proveedores de servicios por los próximos diez años. Implicará el uso de al menos tres arquitecturas de convergencia diferentes como son UMA, IP Móvil y SIP, y una variedad de tecnologías de radio. IEEE 802.11 y las extensiones de este estándar formarán la tecnología dominante en la LAN. En la WAN inalámbrica, serán implementadas una variedad de soluciones móviles como son HSDPA, EV-DO y WiMAX. Las tres deberían progresar muy bien. Apueste, será un mundo inalámbrico.

Steve Hratko es manager de desarrollo de nuevos productos en el Mobile Wireless Group de CISCO. Tiene más de 20 años de experiencia en la industria y ha trabajado con service providers (mayormente operadores móviles) y empresas desarrollando tecnología de voz y datos. Se lo puede contactar en shratko@cisco.com



TECNOLOGÍA PARA EXPERTOS

SUSCRIPCIÓN $70 ANUALES

- **12 EJEMPLARES NEX IT** EN TU DOMICILIO.

- **WEB HOSTING PROFESSIONAL,UN AÑO GRATIS**
100 MB DE ESPACIO,
1GB DE TRANSFERENCIA,
5 CUENTAS POP3/IMAP/WEBMAIL,
10 REDIRECCIONAMIENTOS DE MAIL,
1 CUENTA FTP,
ESTADISTICAS DE VISITAS,
EXTENSIONES DE FRONTPAGE 2002,
PANEL DE CONTROL.

- **CD ANTIVIRUS PANDA**
PLATINUM INTERNET SECURITY 2005 FULL POR 6 MESES

suscripciones@nexweb.com.ar
+54 (11) 5031-2287
NEXWEB.COM.AR

Promoción válida solamente para la República Argentina;
hasta el 31 de Diciembre de 2005 o agotar stock de 150 unidades

Microsoft

Usted construye
la infraestructura.

La infraestructura
construye la compañía.

Windows Server System lo ayuda a que usted y su compañía alcancen sus objetivos de manera más rápida y sencilla. Windows Server System le permite:

Comunicarse y Colaborar externa e internamente.
Integrar los procesos y aplicaciones de su empresa.
Analizar la información de su negocio.
Administrar y Operar su infraestructura tecnológica.

En el mundo de hoy, en el que las demandas de IT cambian constantemente, las empresas exitosas son las que pueden construir soluciones de manera más rápida. Hoy más que nunca esas compañías están construidas sobre Windows Server System.



© 2005 Microsoft Corporation. Todos los derechos reservados.

Un vistazo a Voice over IP

Traducción: **Marcelo C. A. Romeo**

¿Por qué debería interesarme el tema de Voice over IP (VoIP)?

Antes del arribo de la tecnología de voz sobre IP, se necesitaban redes aisladas para transportar simultáneamente tráfico de voz y datos. Ambas redes operan actualmente con el mismo tipo de cableado, pero la infraestructura física de la red de datos ha sido optimizada para hacer uso de voz sobre IP. ¿Por qué? Porque el tráfico de voz, cuya existencia se remonta a mucho más atrás en el tiempo que la del tráfico de datos, comenzó a ser tenido más en cuenta.

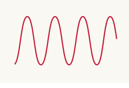
A lo largo de los últimos 20 años, el volumen en el tráfico de datos se ha ido incrementando exponencialmente.

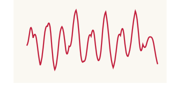
Varios y recientes estudios demuestran que el tráfico de datos supera hoy día ampliamente el tráfico de voz.

Vistas las limitaciones y altos costos del ancho de banda como recurso, hay una constante presión por hacer un uso más eficiente del mismo. Y está probado que una de las mejores formas de alcanzar esta eficiencia, se logra a través de la unificación de las redes de transporte de voz y datos. Dicha convergencia también reduce costos operativos, ya que sólo se hace necesario el soporte y mantenimiento de una sola red. Y dado el mayor uso que están teniendo las redes de datos, se hizo más práctico modificar las señales de voz para que pasarán a través de estas redes que viceversa.

¿Qué inconvenientes se presentan?

En primer lugar, las señales analógicas de voz deben ser convertidas a señales digitales. Todos los sonidos (incluyendo el habla) son ondas analógicas compuestas por una o más frecuencias.


Tono Puro

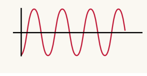

Alguien gritando "Ah!"

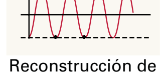
En redes VoIP, estas señales analógicas deben ser convertidas en paquetes digitales antes de ser transportadas a través de las redes de datos IP. Una vez llegados a destino, estos paquetes deben ser nuevamente vueltos a su estado original de ondas de sonido analógicas para poder ser escuchados por el receptor.

Los paquetes deben ser transportados en tiempo real. La calidad del sonido VoIP está basada en la habilidad de la red para despachar paquetes con una alta tasa de transferencia (99% o más), con un delay mínimo (menos de 150 mseg end-to-end). Existen estándares ya establecidos en lo que a calidad respecta. Si bien hay usuarios de VoIP dispuestos a tolerar una baja calidad de sonido a cambio de poder comunicarse a largas distancias, en lo que hace a las aplicaciones comerciales, empresariales y de negocios, la calidad del servicio de VoIP debe al menos igualar a la de la telefonía tradicional.

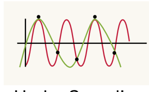
Conversión de voz analógica a digital

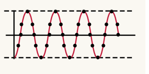
Las señales analógicas están compuestas por formas de onda que varían constantemente en un infinito número de estados, y, en teoría, pueden ser replicadas con exactitud. En lo que hace a la telefonía digital (incluyendo VoIP), la señal original debe ser convertida en un flujo de datos digitales (o serie de paquetes) por parte del transmisor, y devueltos a su estado original una vez llegados a destino por parte del receptor. La conversión analógico-digital es posible gracias al muestreo (sampling): la captura instantánea de medidas de una señal digital. Si se recogen suficientes muestras (samples), la señal original puede ser restaurada a partir de los puntos que corresponden a esas muestras.


Señal Analógica


Reconstrucción de la señal analógica a partir del muestreo (sampling)

Para restaurar correctamente la señal original, hace falta un número suficiente de muestreos. En caso de ser escasos (under-sampling), puede suceder que más de una señal se ajuste a la conexión de los puntos. Si, por el contrario, el número de muestreos es demasiado alto (over-sampling), estaremos a menudo consumiendo más CPU, recursos y ancho de banda sin que esto implique una mejora sustancial en la calidad de la señal.


Under-Sampling

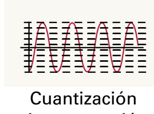

Over-Sampling

El grado de muestreo ideal para cualquier señal es de dos veces la frecuencia más alta que ésta pueda tener. Así, una señal cuya frecuencia es de dos ciclos por segundo, podrá ser perfectamente restaurada realizando cuatro muestreos

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.



por segundo. A esto se lo denomina Tasa de Nyquist (Nyquist Rate), en honor al Ingeniero de los Laboratorios de AT&T que hizo el descubrimiento. El teorema de Nyquist afirma que cualquier señal analógica puede ser recreada digitalmente haciendo un sampling equivalente a dos veces la frecuencia más alta contenida en dicha señal. Usualmente, las señales son sampleadas un poco por encima de la tasa de Nyquist.

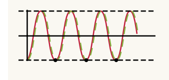


Cuantización sin compresión

Cuantización con compresión

Compresión de voz

Un tema clave en lo que tiene que ver con VoIP, es el uso moderado del ancho de banda. Dada la gran cantidad de información de ruteo contenida en los paquetes de VoIP, se hace necesario comprimir los datos de voz tanto como sea posible. Para esto, existen tres niveles de compresión. El primer nivel consiste, simplemente, en no transmitir aquello que no puede ser escuchado. Una conversación típica es, en su mayor parte, silencio puro. Esto es increíble, pero real. Así, las partes silenciosas de la conversación no son transmitidas. El segundo nivel de compresión consiste en sacar la mayor parte posible fuera de la conversión analógica-digital. Mientras que una señal analógica tiene, como hemos dicho, un número infinito de estados, la representación digital de la misma será una serie de ceros y unos, limitados a su vez por el número de bits empleados a tal fin. Más bits significan mejores niveles de calidad, pero también implica mayor uso de ancho de banda. Por ejemplo, una señal de 8-bits representa 256 niveles. Cada muestra tomada durante el proceso A/D, estará representada por uno de estos niveles. Esto recibe el nombre de cuantización (quantization). Mediante la utilización de varios niveles a bajas amplitudes, se hace posible usar menos bits para obtener la misma calidad de audio que, de otra forma, hubiera requerido un número elevado de niveles y, por consiguiente, mayor requerimiento de ancho de banda.



Señal correctamente sampleada, con una recreación aproximada.

El tercer nivel de compresión consiste en no transmitir los datos de voz, ya que las señales de voz también pueden ser moduladas usando el "pitch" y el "tono". Existen muchas variantes de pitch y tono, y sus valores se pueden almacenar en una tabla. Modernas técnicas de cómputo permiten transportar estos valores para volver luego a recrear las señales originales desde las mismas tablas una vez llegados a destino.

Ruido confortable

Las señales digitales utilizadas por VoIP suelen ser mucho más "limpias" que las señales analógicas usadas en la telefonía tradicional. Porque tratándose de señales analógicas, al amplificar las mismas también se amplifica el ruido (esa estática que muchas veces escuchamos de fondo durante una conversación telefónica). Pero gracias a las señales digitales, el ruido es anulado completamente, ofreciendo un sonido mucho más puro. Y aunque esto puede parecer una ventaja a primera vista, también puede causar ciertos inconvenientes. Y esto es porque en las comunicaciones de voz analógicas, un mínimo ruido de fondo nos garantiza una buena conexión. La mayor parte de los usuarios de telefonía tradicional están acostumbrados a dicho ruido, y al hacer uso de la telefonía IP en medio de una conversación, se preguntan muchas veces si la conexión aún sigue viva, debido justamente a la ausencia absoluta de ruido de fondo. Debido a ello, algunos sistemas digitales "inyectan" estática (conocido esto como "ruido confortable"), como una manera de informar, tanto al transmisor como al receptor, que la conexión es buena en todo momento. ■



No compartido o virtual.
Verdadero servidor dedicado.
Completo acceso root.
No contratos.
Solo por DomainGurus.com

12:45 Have a new dedicated server with a P4 HyperThreading, 1GB RAM, 80GB SATA, and unlimited bandwidth for only $59/mo.

12:52 Get back to online poker.



3.0GHz Intel P4 HyperThreading,
1GB RAM, 80 GB SATA Disco Duro,
Transferencia ILIMITADA
(10Mbps Cisco-Switch Bandwidth = 3200GB por mes)



La telefonía empresarial está cambiando hacia IP



Cómo ven el desarrollo de la telefonía IP en el país? Se puede cuantificar su crecimiento respecto a años anteriores?

De acuerdo a la última encuesta de telefonía IP en el mercado Argentino realizada por la consultora Price & Cooke, se refleja que en Argentina la adopción de Telefonía IP está creciendo a los niveles mundiales y por tratarse de un mercado emergente, las cifras de crecimiento locales podrían superar a las globales en los próximos años. De acuerdo a la encuesta, la adopción de Telefonía IP (entre aproximadamente 130 empresas de entre 200 y 500 empleados), no llegaba al 5 % en el 2004, creció a casi el 20 % en el 2005 y se espera que supere el 40 % en el 2006.

Desde Cisco vemos que la adopción de Telefonía IP está acelerándose mes a mes. Una prueba de ello es que a nivel mundial cada vez tardamos menos tiempo en vender cada nuevo millón de teléfonos (ya despachamos 6 millones en todo el mundo). El primero lo vendimos en 3 años y el último millón en sólo 4 meses. Particularmente en Argentina, la venta de Telefonía IP (en realidad para nosotros tiene un alcance más amplio y la llamamos Comunicaciones IP porque abarca también Video llamadas, Centros de contacto, etc.) ha crecido aprox. 130 % de año a año al cierre de nuestro último año fiscal.

Por otra parte, el mercado mundial total de Telefonía Empresarial -de acuerdo a un estudio de la consultora Synergy Research Group (Fig.1)- se mantiene constante o levemente decreciente. Si lo analizamos en detalle, vemos que las ventas de PBX tradicionales y sistemas de telefonía pequeños denominados KTS (Key Telephony Systems) están decreciendo y lo único que crece es la venta de telefonía IP. Este decrecimiento está sustentado por los anuncios recientes de la mayoría de los fabricantes de telefonía tradicional, los cuales declararon el End of Sale de sus PBX tradicionales o anuncios de ninguna mejora a futuro para dichos modelos.

Pensamos que la adopción de Telefonía IP continuará acelerándose, debido a que por ejemplo ya hay 39 millones de ports de switches Ethernet/Fast/Giga con capacidad de POE Power Over Ethernet), lo cual facilitará la adopción de está tecnología de comunicación. Recordemos que cuando comenzamos con nuestra visión sobre Telefonía IP en el año 1999, no había un standard para POE y la única aplicación que requería POE era la Telefonía IP, con lo cual el ROI de reemplazar el equipamamiento para las Redes LAN era más difícil de obtener. Gracias a la estandarización actual de POE, muchos dispositivos hacen uso de esta funcionalidad como cámaras de video para vigilancia, sensores de RFID, Access Point de Wireless, etc.

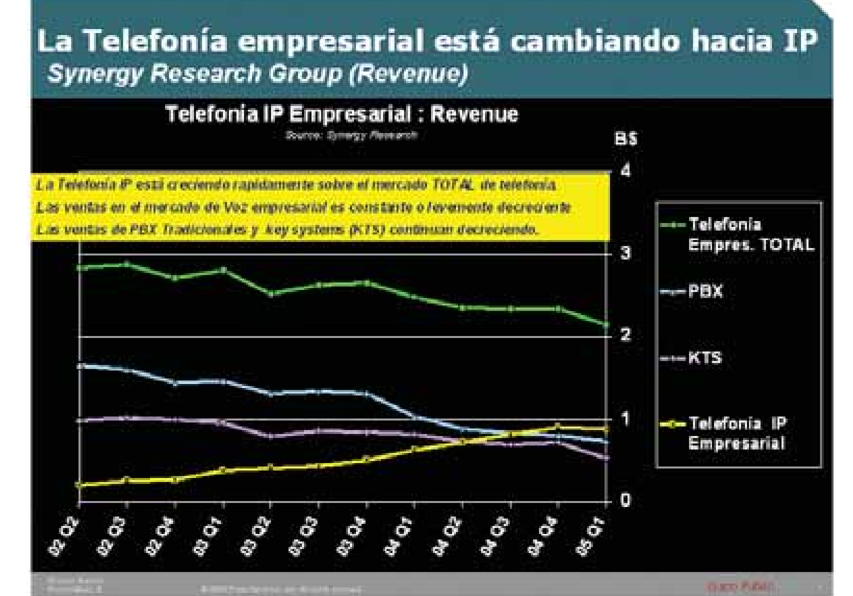


Fig. 1 Estudio de la consultora Synergy Research Group

Cómo ven el desarrollo futuro del tema, habrá una migración a VoIP?

Cabe aclarar que VoIP y Telefonía IP son conceptos diferentes que algunas veces se confunden también con Voz Sobre Internet. A continuación detallo las tres definiciones:

- VoIP: Transporte de Voz encapsulada dentro de paquetes de datos, utilizando el Protocolo de Internet (IP), sobre redes públicas o privadas. Es el cimiento de las comunicaciones IP, pero como simple transporte hace poca diferencia en comparación con otras tecnologías.
- Voz sobre Internet: Se refiere a la posibilidad de realizar llamadas telefónicas, cursando el tráfico sobre Internet en vez de la red telefónica pública conmutada, PSTN. En general es solamente entre dos puntos, requiere una PC, un cliente de software en ambos extremos (el mismo), utiliza mecanismos propietarios para la señalización entre las puntas, no ofrece garantía (ni calidad) de servicio, es altamente inseguro, y no tiene las facilidades para ser atractivo para las empresas.
- Telefonía IP: Sistema avanzado de comunicaciones empresariales, que utilizando IP como medio de transporte, permite crear un sistema telefónico con todas las funciones de un PBX tradicional, y agrega nuevas funcio-

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

nalidades como integración de aplicaciones vía XML, distribución inteligente de la fuerza de trabajo, automatización de la administración, movilidad, etc.

En el caso de Argentina, hay otro factor sumamente importante que está favoreciendo la adopción de Telefonía IP que es el momento actual de la industria de los Call/Contact Centers. Los Contact Centers representan hoy para Argentina una de las industrias que mayor empleos generó en nuestro país, casi al mismo nivel que la industria automotriz o el supermercadismo. La industria facturó $150 Millones durante el transcurso del año 2004. Dicha cifra representa un crecimiento anual mayor al 300% ya que en 2003 facturó $45 Millones y el año precedente $15 Millones. Los servicios de agentes del Call / Contact Center, que puede estar ubicado remotamente con respecto al cliente que está atendiendo, son brindados de manera natural por la telefonía IP y esta industria también está migrando rápidamente sus plataformas tradicionales seducidas por las ventajas evidentes que ofrece esta tecnología.

Cuál es la estrategia/solución de Cisco?

Cisco entrega una solución completa de Comunicaciones IP, compatible con lo que las empresas ya tienen instalado. Entre más híbrida sea la infraestructura y menos IP, menores son los ahorros, menor la funcionalidad, menor la flexibilidad y menor la inteligencia del sistema de comunicaciones. La compañía ofrece una solución de comunicaciones IP que consiste en un sistema amplio de soluciones de clase empresarial incluyendo telefonía IP, comunicaciones unificadas, comunicaciones ricas en medios, incluyendo audio, web y videoconferencia, IP video broadcasting y soluciones de contacto con el cliente que toman ventaja de la infraestructura IP de Cisco del cliente existente para entregar aplicaciones convergentes.

Adicionalmente creemos que la telefonía IP no es una aplicación que se instala sobre la red IP de las empresas sino "en" la red de las empresas por lo tanto se integra naturalemente a la estrategia de seguridad que hemos diseñado , denominada "Redes que se autodefienden", en el cual todos los dispositivos de la red tienen un altísimo grado de seguridad y a la vez colaboran para que la red se comporte como una sola entidad para reaccionar automáticamente a ataques de todo tipo y adaptarse para rechazarlos.

Cuáles son las ventajas y desventajas de la telefonía IP? Y concretamente, en términos de ahorro de costos, se pueden realizar estimaciones de cuánto puede ahorrar una empresa y un usuario particular usando esta telefonía?

En resumen, con respecto a las ventajas que los clientes ven en Telefonía IP, comprobamos que la mayoría toma la decisión de migrar, considerando los ahorros de costos en llamados de larga distancia (Toll ByPass), costos de mantenimiento y administración de redes separadas, pero luego de usar la nueva tecnología observan las ventajas adicionales como movilidad, mejoras en la productividad de los empleado, mejor colaboración entre empleados (Video Conferencia, RichMedia, etc), ventajas competitivas en el sentido de poder responder mejor y más rápido ante las necesidades de los negocios, mejor fortaleza del negocio, por mejorar la recuperación ante problemas o desastres, etc.

El ahorro de cada implementación depende de la situación particular de cómo llega cada empresa a la implementación de Comunicaciones IP, pero en resumen podemos mostrar un gráfico promedio de aumentos de productividad que observaron varios clientes que hicieron ya la migración (fig.2) ■

Telefonía IP: Beneficios reales

Beneficios de la Telefonía IP	En números..
Aumenta productividad de empleados en oficinas remotas	4.3 horas por trabajador remoto por semana o 28 días (aprox. 12%) por año.
Aumenta productividad de Teletrabajadores	5 horas por semana o 33 días (aprox. 14 %) por año.
Reducción en gastos de viaje para IT	13 horas por mes por empleado de IT o 19 días (aprox. 9 %) por año.
Mayor rapidez en cambios, adiciones y movimientos (MACs)	1.5 horas menos por movimiento.
Aumenta productividad de usuarios finales y de IT debido a facilidad de uso	5.5 horas por semana (aprox. 16 %) por empleado de IT involucrado en soporte telefónico.
Facilita cambios, adiciones y movimientos a empleados	3 movimientos más por año por empleado.
Reducción del tiempo requerido para localizar a una persona en el teléfono(telephone tag).	3.9 horas por semana por empleado o 25 días (aprox. 11 %) por año.

A partir de una encuesta a 100 organizaciones que utilizan Telefonía IP, Sage Research & BCR, Julio 2003

Fig. 2 Telefonía IP: Beneficios reales.



Fabián Dominguez
Gerente de Desarrollo de Negocios de Tecnologías Avanzadas de Cisco Systems en Sudamérica Sur.



Gráfico soporte, mercado teléfonos IP en Argentina

Transformación a Redes IP NGN en los Proveedores de servicios

La innovación de Cisco y sus avances en tecnología están ayudando a los proveedores de servicios en la transformación hacia las redes de la próxima generación basadas en IP.

Lejos están los días cuando proporcionar conectividad era el nombre del juego. Hoy, los proveedores de servicios de toda clase deben apuntar a ofrecer servicios nuevos, de valor agregado para el crecimiento de los ingresos, mayor diferenciación competitiva, e incrementar la lealtad del cliente. Estos han adoptado un enfoque estricto en lograr eficiencia en los gastos operacionales (OpEx) e inversiones de capital (CapEx) para mejorar la rentabilidad. Y en este ambiente intensamente competitivo, es cada vez más importante para los proveedores ganar control de sus redes y los servicios que corren en ellas y, en el proceso, recobrar el control de su negocio en el mercado cambiante.

Los proveedores de servicios también necesitan soluciones flexibles que los ayuden a cubrir los requerimientos económica y eficazmente, y tomar las oportunidades de los distintos segmentos de sus clientes - consumidores, pequeñas y medianas empresas, empresas grandes, y clientes mayoristas. Por ejemplo, en el espacio del consumidor, soluciones como juegos (gaming), videograbadoras personales basadas en la red (NPVR), video en demanda (VoD), redes inalámbricas Wi-Fi, y la movilidad son áreas de importante crecimiento. Las pequeñas y medianas empresas es probable que aumenten su interés y uso de un rango de servicios gestionados como hosting y seguridad. Entretanto, las grandes empresas experimentarán una demanda incrementada de redes privadas virtuales Layer 2 y Layer 3 (VPNs), acceso remoto, almacenamiento, y seguridad, incluyendo servicios de conexión Ethernet. Por su parte, los proveedores de servicios buscarán rédito también en la venta de acceso al por mayor, la voz local y de larga distancia, y servicios que incluyen la colocación, peering, transporte, y entrega del contenido.

Para dirigirse a estos mercados diversos, los proveedores necesitan una sola infraestructura capaz de evolucionar para proporcionar una gama amplia de nuevos servicios que aumentarán las ganancias y la lealtad del cliente, como así también producir eficacias en OpEx y CapEx. La industria generalmente llama a esta infraestructura de avanzada como redes de la próxima generación (NGN – Next Generation Networks) y tiene el consenso unánime de que IP será la tecnología de base para hacerla realidad.

Muchos en la industria han definido el término NGN para dirigirse sólo a un pedazo pequeño de la transición requerida por los proveedores de servicios. Cisco toma una visión más integral de una NGN basada en IP que se dirige a una gama amplia de aspectos que los proveedores de servicios deben resolver. Nosotros creemos que las IP NGN provocan una transformación de red amplia que no sólo abarca la red del proveedor de servicios sino también su negocio en conjunto.

Esta transformación de red no termina en un solo punto. La IP NGN es un continuo, así como los planes de servicio y el negocio en general de los proveedores. Constantemente evolucionará para adaptarse a la demanda del cliente y a las nuevas oportunidades.

Las redes IP NGN se refieren a la idea de una red que no sólo puede económica y eficazmente entregar y manejar todas las opciones de comunicaciones de voz, de video, y de datos disponibles hoy, sino que también puede adaptarse y crecer para manejar cualquier nueva opción de comunicaciones que inevitablemente evolucionará.

Muchos proveedores de servicios ya están trasladándose a IP NGNs. Aunque

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.



ellos podrían usar términos diferentes para NGN, hablando en forma general, comparten muchos de los conceptos básicos en sus visiones para la infraestructura del proveedor del mañana.

El desarrollo escalonado de la IP NGN involucra crear una infraestructura inteligente desde la cual los servicios sean concientes del tipo de aplicaciones (application-aware services) y sean entregados por redes que sepan de esos servicios (service-aware network). Este tipo de IP NGN inteligente abrirá nuevas oportunidades a los proveedores para ofrecer a sus clientes finales servicios avanzados, de valor agregado, personalizados y transparentes sobre conexiones tanto alámbricas como inalámbricas.

La Convergencia está en el Corazón de la IP NGN

En el centro de la IP NGN hay tres áreas fundamentales de convergencia que ya están siendo habilitadas hoy por los proveedores de servicios:

- ***Convergencia de aplicación***— integrando aplicaciones nuevas e innovadoras de datos IP, voz y video sobre una única infraestructura de banda ancha.

- ***Convergencia de servicios***— Los proveedores están emigrando hacia la entrega de servicios "Triple Play on the move", que combina servicios de voz, video, datos, y movilidad. La convergencia de estos servicios incluye el control y acceso a la red que es indiferente a la tecnología utilizada y compatible transparentemente con cualquier medio de conectividad: Cable, DSL, Ethernet, inalámbrico, o móvil.

- ***Convergencia de red*** — Los proveedores están migrando de desplegar, manejar, y mantener redes específicas de servicio múltiples a entregar todos los servicios en una sola red, cada vez más a menudo a una única red basada en IP MPLS (IP Multiprotocol Label Switching).

Por supuesto, los proveedores de servicios priorizan estas áreas de convergencia de maneras diferentes, dependiendo de su negocio. Por ejemplo, muchos operadores de móviles podrían enfocar la mayoría de sus esfuerzos en la convergencia de servicios, mientras que los operadores de cable apuntan sus esfuerzos a la convergencia de aplicaciones. Sin embargo, el punto común es que todos requieren de la convergencia de red para ser rentables en el mercado competitivo.

La visión y la arquitectura de la IP NGN de Cisco tratan estas tres áreas primarias de convergencia (véase la figura 1).

Los recientes avances de Cisco, mayor-

mente en las áreas de control de servicio y la capa de aseguramiento de la red, subrayan su compromiso en desarrollar la tecnología y las soluciones que ayuden a los proveedores de servicios a transformar sus redes en IP NGNs comercialmente provechosas.

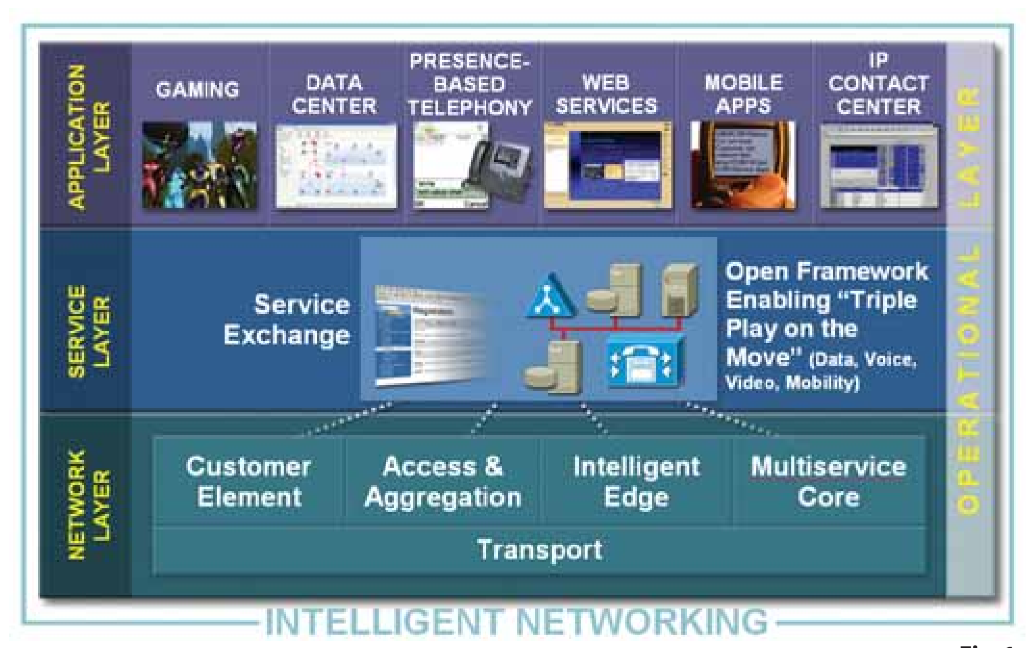


Fig. 1

Cisco IP NGN: Capa de Control de Servicio (Service Control Layer)

Para lograr una convergencia real de servicios, las compañías deben ser capaces de operar, gestionar y facturar servicios dentro de una variedad de medios de acceso. Con este propósito, Cisco y sus partners en tecnología han desarrollado y siguen avanzando en la implementación del Marco de Intercambio de Servicio abierto (Service Exchange Framework), el cual permite a los proveedores facilitar y controlar el acceso de los clientes y el uso de servicios IP de accesos de medios fijos y móviles sin límite en los tipos de aplicaciones a desplegar.

Mientras que este marco incluye una variedad de diferentes productos y soluciones de Cisco y sus partners, una de sus más recientes incorporaciones proviene de la adquisición de P-Cube por parte de Cisco, que es un desarrollador de plataformas de control de servicios IP.

La solución Cisco Service Control reviste a las ya existentes redes de transporte IP con controles de niveles de aplicación e inteligencia, permitiendo que los proveedores de servicio analicen, controlen , midan y facturen servicios en base a contenido y aplicaciones múltiples - todos sobre una infraestructura de red común. Los componentes de hardware de la solución, los Cisco SCE 1000 y 2000 Series Service Control Engines, son elementos programables de la red que se encuentran, por ejemplo, detrás de un dispositivo de agregación como el Cisco 10000 Series Router, servidor de acceso remoto a banda ancha (B-RAS), o sistema de terminación de Cable Momem (CMTS). El SCE Cisco interopera tanto con componentes de gestión y autenticación de abonados como con sistemas de recolección de datos, facturación y sistemas de políticas de aprovisionamiento, todo esto para ofrecer a los abonados servicios de banda ancha transparentes y de aplicaciónes diferenciadas.

El conjunto de aplicaciones de Control de Sercivios (Cisco Service Control Application Suite), que funciona en los motores de control de servicio, esta compuesto por tres aplicaciones de software: Aplicación de Control de Servicio (Service Control Application) para el monitoreo del servicio del abonado, aplicación para Gestión de Recolección (Cisco Collection Manager) para la captura y la transmisión de los datos del servicio, y la aplicación de Gestión de Abonado (Cisco Subscriber Manager) para el control y la contabilización del tráfico individualizado. El Service Exchange Framework se encuentra aún más enriquecido por la reciente adquisición, por parte de Cisco, de dynamicsoft, un realizador de software de voice-over-IP (VoIP) basado en Session Initiation Protocol (SIP). La integración de la tecnología de dynamicsoft con los productos VoIP de Cisco, tales como el Cisco BTS 10200 Softswitch, permitirá a los proveedores brindar servicios de comunicación integrados basados en SIP (teléfono, teléfono movil, e-mail, mensajería instantánea, etc.) haciendo posible que los usuarios sean contactados a través de un único dispositivo.

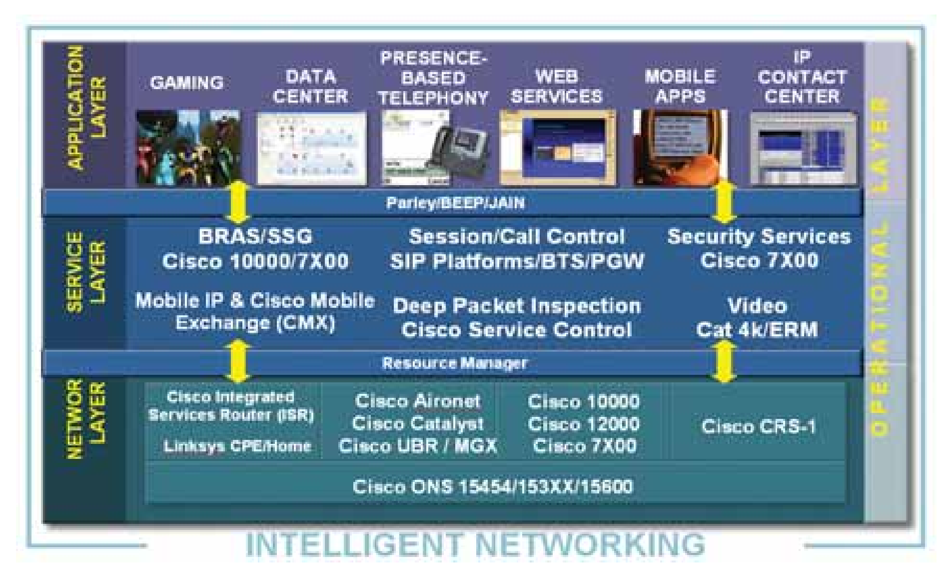
Estos nuevos componentes del Service Exchange Framework complementan tambien el portfolio de Cisco Mobile Exchange (CMX) existente para operadores móviles, el cual está dirigido a la interface entre la red de acceso de radio y el conjunto de servicios de Internet ofrecidos por las redes IP. El CMX da a los operadores móviles, los proveedores de aplicaciones, y los integradores de sistemas, soluciones flexibles que les permitirá brindar servicios de datos de valor agregado a sus abonados móviles.

Cisco IP NGN: Capa de Red Segura (Secure Network Layer)

La base de la IP NGN es la capa de red, compuesta por los elementos del cliente, los de acceso/agregación, el borde IP MPLS inteligente, y los componentes centrales de la red multiservicio. Todos ellos sobre la capa de transporte y con interconexiones con los elementos de las capa superior. La capa de red segura se encuentra atravesando una serie de cambios fundamentales en comparación a años anteriores. Por ejemplo, el IP MPLS esta siendo integrado a través de cada sección de la red, y las áreas centrales y periféricas están en proceso de convergencia, cada una de las cuales se encuentra adoptando capacidades de la otra y otorgando mayor eficiencia a los



Damian Mauro
Global Systems Engineer
Service Providers - Latin America
CCIE #9485



Las instituciones de investigación y los proveedores globales en todo el mundo están en proceso de adopción del Cisco CRS-1 para la construcción de sus infraestructuras de red IP y para el envío de servicios multimedia de avanzada.

proveedores de servicios.

Cisco ha jugado un papel preponderante en el desarrollo de las infraestructuras de comunicaciones IP MPLS, la base para redes IP convergentes a larga escala de última generación. Durante varios años, IP MPLS ha sido reconocido como el habilitador fundacional de la convergencia de red. Cisco tiene más de 250 clientes de proveedores de servicio en todo el mundo que despliegan IP MPLS. Cisco lidera la industria en la creación de tecnología innovativa para impulsar la convergencia de redes y para permitir que los proveedores de servicios logren bajar sus costos de infraestructura. Esto se evidencia claramente con el nuevo Cisco CRS-1 Carrier Routing System y con el recientemente lanzado CRS-1 8-Slot Single- Shelf System. El sistema de ruteo más avanzado del mundo, el CRS-1, tiene una capacidad de sistema de hasta 92 Terabits por Segundo (Tbits/s) y está diseñado para proveer una operación continua del sistema, flexibilidad en el servicio, y longevidad extendida del sistema para proveedores de telecomunicaciones e instituciones de investigación. Diseñado para adecuarse a la mitad de un rack standard de 19 pulgadas y con una capacidad total de conmutacion de 640 Gbit/s, el Cisco CRS-1 8-Slot System prolonga el alcance del CRS-1, brindando una base para la convergencia de redes y servicios.

Mapa de productos para cubrir las áreas primarias de convergencia de la IP NGN

La estrategia de Cisco en el campo de los proveedores de servicio consiste en innovar y en proveer la tecnología, las soluciones, y el profesionalismo que los carriers requieren a medida que estos transforman sus redes y se trasladan a través del viaje hacia la IP NGN. El despliegue de soluciones que ofrecen una mayor inteligencia de red, integración, y flexibilidad global no solo proveerá a los carriers con un remedio a corto plazo, sino que también les permitirá, finalmente, combatir las presiones competitivas, apuntar a nuevas oportunidades de mercado, y, consecuentemente, aumentar la rentabilidad. ■

LECTURA COMPLEMENTARIA

- Informacion de vision y arquitectura de Cisco para redes IP NGN:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns301/c654/cdccont_0900aecd801d71ed.pdf
- Informacion de plataforma de Control de Sesión (Cisco Call Session Control Platform):
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns311/c654/cdccont_0900aecd802716f7.pdf
- Informacion de Cisco Mobile Exchange:
http://cisco.com/en/US/netsol/ns341/ns396/ns177/ns278/networking_solutions_package.html
- Control de Servicio Cisco (Cisco Service Control)
http://www.cisco.com/en/US/products/hw/cable/products_promotion0900aecd801cac91.html
- Sistema de Ruteo Carrier Cisco CRS-1 (Cisco CRS-1 Carrier Routing System)
http://www.cisco.com/en/US/products/ps5763/index.html
http://www.cisco.com/en/US/products/ps5763/index.htmlADING
- Soluciones de Ruteo para Proveedores de Servicio.
http://www.cisco.com/en/US/products/hw/routers/index.html





Redes Autodefensivas

Gastón Tanoira, Gerente de Soluciones de Seguridad de Cisco para América Latina, habla sobre la estrategia de Seguridad de Cisco, las razones que llevan a las empresas a implementar estas soluciones y cómo deben afrontar su seguridad de redes.

¿Cuáles son los elementos claves de la estrategia de seguridad de Cisco?

La estrategia de seguridad de Cisco está basada en el concepto de Red Auto-Defensiva, que significa que la red tiene la habilidad de identificar, prevenir y adaptarse a las amenazas de seguridad. Cisco entiende que la única defensa viable a los ataques modernos de seguridad, debido a su complejidad y rapidez de expansión, es mitigar estos riesgos en la propia red. No se puede depender de dispositivos puntuales que estén en la periferia sino que la red en sí misma debe defenderse.

El primer elemento de la estrategia de seguridad de Cisco es la Integración. La seguridad de la red debe ser integrada a nivel del sistema. Todos los componentes de la red tienen que ser punto de defensa e interactuar entre sí mismos. Los routers tienen que hablar y trabajar con los switches, los firewalls, los sistemas de prevención de intrusos, servidores, Pcs, los puntos de acceso inalámbricos, etc. Todo debe trabajar como un sistema unificado.

La Colaboración es el segundo de los elementos. Cisco lanzó la iniciativa Control de Admisión de la Red (NAC, por sus siglas en inglés) a la cual se han sumado los principales proveedores de seguridad (Trend Micro, IBM, Network Associates, Symantec, Microsoft), para crear una plataforma donde convergen todas las tecnologías que hacen que las redes sean más seguras. De esta manera se obtiene colaboración entre las empresas, y se tienen dispositivos que trabajan en coordinación para mitigar los ataques.

Como tercer y último elemento está la Defensa que se adapta a las amenazas. Es un enfoque proactivo y no reactivo, donde la red se adapta a la evolución de los nuevos ataques. De esta manera la red puede identificar comportamientos sospechosos de los distintos dispositivos conectados a una red, independientemente que el ataque sea conocido o no.

Cisco concibe la infraestructura de TI como un ser viviente, donde la red es el sistema inmunológico. Los seres vivientes estamos expuestos a virus y enfermedades en nuestra vida diaria, pero a pesar de esto el cuerpo se defiende solo, sin que nos enteremos. En las ocasiones que el virus traspasa las primeras defensas, las funciones vitales siguen trabajando. De esta misma forma las redes deben autodefenderse para proteger sus aplicaciones de misión crítica.

¿Qué factores han llevado a que la seguridad sea hoy un tema tan crucial?

Cada vez más las empresas están usando aplicaciones que son determinantes para el funcionamiento y productividad de sus negocios. El éxito de las compañías, y su supervivencia, dependen de estas aplicaciones y de la productividad que pueden obtener implementándolas. De esta manera, la disponibilidad, la confiabilidad y la integridad de los datos, son fundamentales para el negocio.

En la década de los 80s, los virus que existían, que se propagaban por medio de disquetes, únicamente infectaban máquinas individuales y su velocidad de propagación se medía en semanas o meses. En la década de los 90s, la

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.


todo
bajo
control
poweredbycisco.
Mantenga siempre el control de su empresa
La Red Auto Defensiva de Cisco ofrece un portafolio completo
de soluciones integradas de seguridad, optimizando su capacidad
para identificar, prevenir y responder a las constantes
amenazas que atentan contra su negocio. Con estas
soluciones de seguridad, Cisco y sus partners le ofrecen
la habilidad para reducir sus costos y dar continuidad a su negocio.
Transforme su red en una herramienta estratégica y asegúrese
una ventaja competitiva ingresando a nuestro site para más
información y promociones: **www.cisco.com/offer/seguridadnexit**
o comuníquese al **0810-444-CISCO (24726).**
CISCO SYSTEMS
security. powered by
© 2006 Cisco Systems, Inc. Todos los derechos reservados.

segunda generación de virus se propagaba por medio de email y office macros y se empezaron a registrar incidentes limitados de hackers. El tiempo de propagación de estos ataques se medía en días y semanas y afectaba únicamente redes individuales. Los ataques modernos están basados en gusanos masivos, ataques de negación de servicio distribuidos, spyware, hacking de infraestructura, etc. El impacto es a nivel global y la velocidad de propagación puede llegar a alcanzar cientos de miles de computadores infectados en cuestión de segundos. A su vez, el tiempo que transcurre desde el conocimiento de una vulnerabilidad en un sistema, a la disponibilidad de una herramienta para aprovecharla y hacer daño, se está acortando drásticamente.

Así, la evolución de los desafíos en términos de ataques a la seguridad debido a su mayor complejidad, la rapidez en que se propagan y el incremento en conocimiento y organización que tienen quienes realizan estos ataques, hace que la seguridad ocupe un primerísimo lugar para los directivos de las empresas.

Según Gartner, por ejemplo, en el año 2002 el tema de seguridad de la red ni siquiera aparecía como un tema de preocupación para los directivos de las empresas. En el 2003 ya aparecía como preocupación número 12, y en el año 2004 pasó a ser la preocupación número uno, aún por encima de la optimización de los costos operativos y el crecimiento en ventas.

Además, las empresas están colocando más y más aplicaciones de negocio sobre sus redes. Por ejemplo, están migrando su red de voz a su red de datos; están añadiendo conectividad wireless; están añadiendo sistemas de automatización de producción, logística, facturación, y todo sobre la misma red. Y aquí la seguridad adquiere una nueva dimensión, ya que las compañías cada vez más dependen de sus sistemas informáticos.

¿Cómo deben las empresas afrontar el reto de la seguridad de redes?

Las empresas deben afrontar el tema de seguridad de redes desde cuatro niveles diferentes. En primer lugar, debe haber una definición de las políticas de seguridad y sus procesos. La empresa debe definir cuáles son sus activos más importantes; aquellos que deben resguardar para darle continuidad y éxito a la empresa, y debe enfocar sus recursos para respaldar estos activos. La mayor parte del esfuerzo lo tienen que poner en donde se genera la mayor parte de su negocio.

En segundo lugar, debe haber educación y conscientización de parte del personal en las empresas. Los empleados deben ser conscientes de las consecuencias de su actuar en sus empresas en términos de seguridad.

Como tercer nivel se encuentra la tecnología en sí, que debe ser de tal modo que las empresas puedan guardar sus sistemas de información de manera efectiva, con el fin de requerir la menor participación humana posible. Debe ser autodefensiva y tener la habilidad para adaptarse a las evoluciones de seguridad de hoy y de mañana.

Por último, es vital el gerenciamiento de las plataformas de seguridad. Las empresas deben tener sistemas que faciliten el trabajo al equipo responsable por la seguridad para poder hacer auditorías y confirmar que las personas actúen de acuerdo con las políticas preestablecidas por cada compañía. Es vital que haya un panorama claro del estado de los sistemas, de dónde viene el ataque, qué tipo de ataque es, cómo afecta esto al sistema y cómo poder mitigarlo de la mejor manera posible.

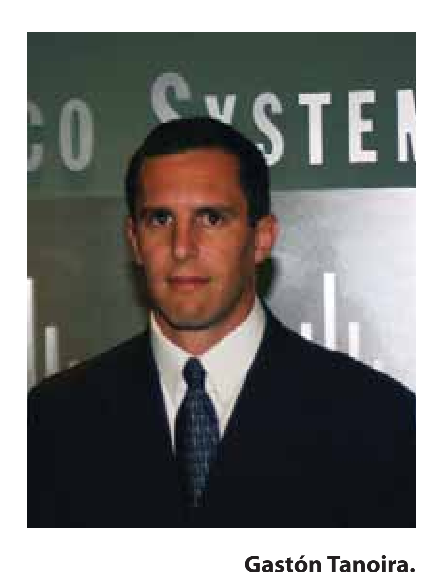
¿Qué está haciendo Cisco en Latinoamérica en seguridad?

La línea de negocio de seguridad de Cisco es una prioridad en América Latina. Cisco está invirtiendo fuertemente en esta línea de negocio, tanto en desarrollo tecnológico, adquisición de recursos específicos para Latinoamérica, como en formar alianzas con las principales empresas que complementen nuestra oferta en seguridad, tanto a nivel global como local. Hoy en día Cisco es el líder en Latinoamérica en participación de mercado en seguridad (según IDC, Cisco tiene el 52% de participación de mercado en dispositivos de seguridad en América Latina).

Somos conscientes de la importancia de este tema para la región y estamos centrando todos nuestros esfuerzos para poder ofrecer a nuestros socios y clientes las herramientas necesarias para enfrentarse a los crecientes ataques a la seguridad.

De acuerdo con la encuesta realizada por Kaagan Research y patrocinada por Cisco Systems, "Actitudes de los Directores de Tecnología de Empresas Latinoamericanas con respecto a Internet: Seguridad", realizada en el 2003, muestra que en lo que más se invertirá es en el tema de tecnologías de seguridad (Un 55% de las empresas dicen que invertirán en seguridad) y la tendencia es totalmente creciente.

Por otro lado hay que considerar que Latinoamérica es una región que de por si está un poco más atrasada en comparación con otras regiones del mundo en términos de adopción de tecnologías informáticas y seguridad. Por esta razón hoy en día en Latinoamérica la inversión de seguridad está creciendo más que en otras regiones. Mientras que el crecimiento a nivel mundial de las inversiones en seguridad se estima que sea del 8.3% anual en los próximos 2 años, en Latinoamérica este crecimiento se estima que sea del 25.2 % en los próximos 2 años. ■



Gastón Tanoira.
Gerente de Soluciones de Seguridad de Cisco para América Latina

TECNOLOGÍA PARA EXPERTOS

SUSCRIPCIÓN $70 ANUALES

- 12 EJEMPLARES NEX IT EN TU DOMICILIO.

- WEB HOSTING PROFESSIONAL, UN AÑO GRATIS
100 MB DE ESPACIO,
1GB DE TRANSFERENCIA,
5 CUENTAS POP3/IMAP/WEBMAIL,
10 REDIRECCIONAMIENTOS DE MAIL,
1 CUENTA FTP,
ESTADISTICAS DE VISITAS,
EXTENSIONES DE FRONTPAGE 2002,
PANEL DE CONTROL.

- CD ANTIVIRUS PANDA
PLATINUM INTERNET SECURITY 2005 FULL POR 6 MESES

Promoción válida solamente para la República Argentina; hasta el 31 de Diciembre de 2005 o agotar stock de 150 unidades

suscripciones@nexweb.com.ar
+54 (11) 5031-2287
NEXWEB.COM.AR





Evolución de los DATACENTERS

Las nuevas tendencias que están impactando en la Arquitectura de Red de los Data Centers.

Autor: **Mauricio Arregoces**
Traducción: **Ing. Marisabel Rodriguez Bilardo**

Las empresas desarrollan objetivos de negocios para controlar los costos operacionales y aumentar la agilidad del mercado, y las tecnologías de avanzada en los Data Centers proveen nuevas maneras para lograrlos. La adopción de tecnologías de avanzada causa una rápida evolución de los Data Centers en las Organizaciones.
Este artículo discute los efectos de las tendencias emergentes en la arquitectura de las redes de Data Centers y los cambios en la arquitectura que influencian a los Data Centers de próxima generación.

Tendencias que están surgiendo

La necesidad de controlar los costos operacionales resulta en la consolidación de varias áreas de tecnología como servidores, aplicaciones, storage y hasta Data Centers. Otras tendencias derivan de buscar niveles más altos de fortaleza y elasticidad, lo que se traduce en las aplicaciones y seguridad de datos, continuidad de negocio, y clusters de servidores en entornos distribuidos. Por ejemplo, las uniones y adquisiciones de empresas ayudan a generar un crecimiento rápido en diferentes mercados, creando la necesidad de compartir aplicaciones y unir redes mientras que se controla el acceso de los usuarios, la autenticación, el ruteo y políticas de seguridad.
La segmentación de la red y las tecnologías de virtualización simplifican este tipo de uniones. Por ejemplo, algunas tendencias resultan del crecimiento y la expansión de las Organizaciones, lo que requiere capacidad de planeamiento ("capacity planning") para poder manejar problemas como pueden ser la alimentación de los equipos, la refrigeración, cableado y flujo de aire, así como también crecimiento de la red y capacidad de cómputo.

Tendencias de consolidación

La consolidación es sin duda la tendencia más común que afecta a los Data Centers en el mundo hoy. Los "drivers" claves del negocio incluyen control de costo, eficiencia operacional, y utilización efectiva de los recursos. La figura 1 ilustra la consolidación de la tecnología en los Data Centers.

Consolidación de los Data Centers

La consolidación de los Data Centers implica que el número de Granjas de Servidores ("Server farms") se reduzca y los servidores se reubiquen en instalaciones existentes o nuevas. Estos Data Centers consolidados están interconectados y las prácticas operacionales, de soporte y diseño están estandarizadas.
Los objetivos de consolidación incluyen que haya menos sitios para administrar, centralización de la estructura de cómputo (servidores y aplicaciones), como muestra la figura 1, y usar el "know-how" que se tiene en los Data Centers existentes. Desde una perspectiva de redes, los entornos consolidados administran una cantidad de servidores significativamente mayor, lo cual requiere una mayor densidad de puertos, un uso mayor de servicios basados en redes, y alta disponibilidad mejorada para poder alcanzar un mayor nivel de exposición. Estos cambios influencian las tasas de "oversubscription" (sobreutilización del ancho de banda), throghput total, escalabilidad y objetivos de alta disponibilidad.

Consolidación de servidores

La consolidación de Servidores implica la reducción de la cantidad de plataformas de harware y sistemas operativos soportados, y la estandarización de los entornos de aplicaciones (niveles web y middleware). La reducción de hardware de servidores permite mayor eficiencia en la reparación de equipos, alivia los problemas de inventario de repuestos, y facilita el mantenimiento así como también reduce la exigencia para los técnicos de hardware. La estandarización del hardware de servidores incluye elegir la tecnología de BUS/NIC (por ejemplo, elegir entre PCI, PCI-X o PCI Express, y entre 10/100, 10/100/1000, y 10 Gigabit Ethernet para la conectividad de servidores), y elegir entre "single" y "multihoming". Las consideraciones de red incluyen revisar las tasas de "oversubscription" entre los servidores y la capa de acceso, entre las capas de acceso y agregación, y entre las capas de agregación y Core; la densidad de puertos necesaria para "multihoming", y el tipo de agrupación de tarjetas de interfaz de red (NIC). Las tasas de "oversubscription" pueden cambiar substancialmente usando PCI-Express y Gigabit Ethernet porque el pomedio de tasas de ráfaga puede incrementarse, y "homing" doble necesita del doble de puertos, así como también adyacencia de capa 2 entre diferentes switches de acceso.

Integración de Servidores Blade (Placas Integradas)

La tecnología de Blade-Server provee mayor capacidad de cómputo, memoria, y capacidad de I/O por rack mientras reduce el cableado (red y "KVM" - keyboard, video and mouse). Los aspectos relacionados a la red que hay que tener en cuenta cuando se integran Blade-Servers incluyen la selección de I/O y Network Fabric (infraestructura de interconexión). Las opciones de I/O son "Pass Through" e "Integrated Network Fabric". La tecnología "Pass Through" conecta servidores directamente a la red, mientras que "Integrated Network Fabric" es un conjunto de switches redundantes dentro del chasis al cual se conectan los servidores. En entornos de "Pass Through", los servidores requieren conexiones externas de cable. Cuando se usa "Integrated Network Fabric", las opciones están entre Ethernet, Fibre Channel e Infiniband, y cada server es pre-cableado a los slots donde están los switches. Los switches integrados proveen varios uplinks para conectar a la infraestructura existente de Data Center.

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

Consolidación de Storage

La consolidación de Storage simplifica la administración de Storage a través de la centralización y mejora la utilización de la capacidad. Migrando de Direct Attached Storage Disks (DASD - Discos conectados directamente a los servidores) a arrays de discos centralizados, la utilización es más eficiente y mejor administrada.

Las tecnologías de Storage Area Networks actuales (SANs), que soportan una alta densidad de puertos de Fibre Channel y separación lógica de SANs (a través de virtual SANs), permite centralizar el storage y consolidar islas de storage mientras que se reducen las infraestructuras de red de storage dispares. Las consideraciones de red incluyen densidad más alta de puertos de Fibre Channel en la capa de borde y de Core para la conectividad de los servidores, de los arrays de storage y el sub-sistema de cintas de backup respectivamente. Consideraciones adicionales pueden ser tratar de lograr un nivel más alto de redundancia y performance para mantener niveles razonables de "oversubscription".

Integración de Aplicaciones Multi-Nivel (Multi-Tier)

La integración de las aplicaciones Multi-Tier comprenden la migración de las aplicaciones basadas en web donde la presentación (web), aplicaciones (middleware - software que une a dos aplicaciones separadas), y funciones de base de datos están desacopladas con respecto al software y físicamente en servidores diferentes. La integración de aplicaciones también incluye el uso de servicios de web, estandarización de entornos de middleware y soporte para Arquitectura Orientada a Servicios (SOA "Service Oriented Architecture"). Los servicios basados en web proveen medios para escalar, mejorar la seguridad, manipular mensajes, y permitir el cacheo de contenido estático y dinámico, así como también archivos de File Systems de red. Las funcionalidades basadas en red son adaptables a las aplicaciones lógicas o físicas tier por tier (nivel por nivel), por aplicación, o por grupo de aplicaciones Multi-Tier. La flexibilidad con la cual los servicios basados en redes se aplican viene de la virtualización de las capacidades, donde el hardware subyacente soporta el uso de instancias lógicas independientes.

Seguridad de Datos y Aplicaciones

La seguridad de datos y aplicaciones se controla tanto en el Data Center como en el resto de la red de la empresa. La seguridad en los Data Centers se enfoca en la integridad, confidencialidad, y accesibilidad de la información mantenida en las granjas de servidores, y se logra mitigando los efectos de los ataques en contra de los servidores, aplicaciones, storage y la infraestructura de red que los soporta.

Seguridad de Servidores y Aplicaciones

La seguridad de servidores y aplicaciones controla la segmentación de las capas de aplicación de las granjas de servidores, la protección contra los ataques de denegación de servicio (DoS - "Denial of Service") y denegación de servicio distribuida (DDoS) y la protección contra Worms. Para lograr el rango de requerimientos, los servicios basados en red usan agentes que corren en servidores que protegen específicamente los entornos de aplicación y los dispositivos de servicio y que monitorean y analizan el tráfico incluyendo información correlativa de múltiples dispositivos para reducir los falsos positivos. Los servicios basados en redes incluyen dispositivos de detección y protección contra intrusos, dispositivos de protección contra DoS, firewalls, análisis de tráfico, y "correlation engines" (encargados de analizar en tiempo real las transacciones de los usuarios que atraviesan la red).

Seguridad de Datos

La seguridad de datos involucra proteger información que está contenida en arreglos de discos, tanto si están conectados a una red IP o a una SAN (Storage Area Network), o se mantienen conectados directamente a los propios servidores (DASD). Dos de los objetivos principales

CONSOLIDACIÓN DE RECURSOS EN EL DATA CENTER

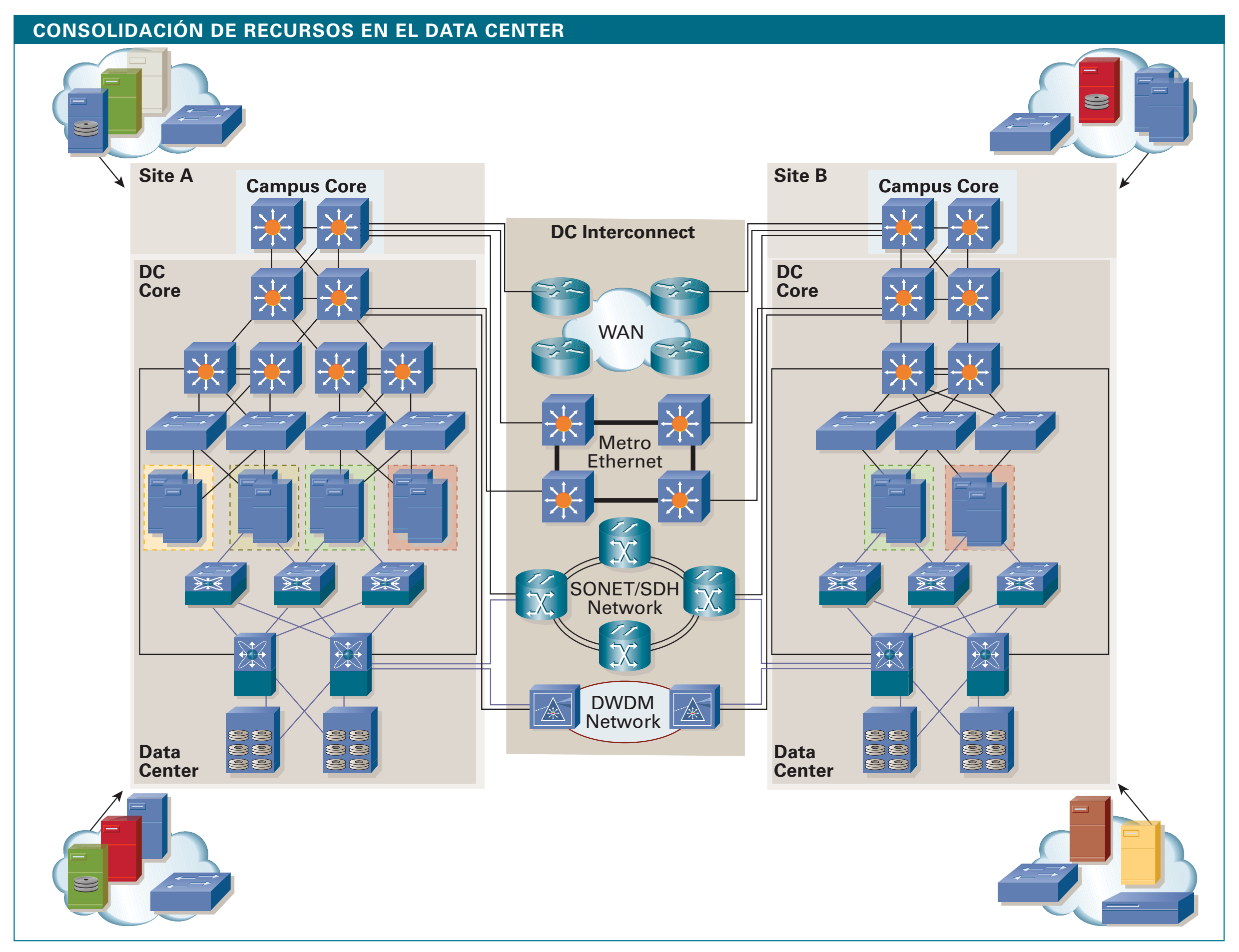


FIGURA 1
La consolidación de recursos en data centers implica una mejor distribución de clusters de servidores, y la reubicación de servidores en las ya existentes o en nuevas instalaciones.



son mantener la integridad de datos evitando la alteración de los mismos y también evitar el robo. Cuando los datos se mantienen en la red IP (NAS o DASD), aplican los mismos mecanismos de protección usados en los servidores y aplicaciones. Cuando la información se guarda en arrays de storage, los mecanismos de seguridad están dados por la infraestructura de red dividida en zonas, y la autenticación y seguridad están basadas en puertos. En casos donde los datos se guardan en SAN pero son transportados por IP (FCIP o iSCSI) como en replicación de datos o backup remoto, las medidas de seguridad, como encripción y redes privadas virtuales (VPNs), se aplican para aislar o segmentar y encriptar los datos en tránsito.

Infraestructura de Seguridad

La infraestructura de seguridad involucra proteger los dispositivos de red y links que soportan tráfico desde y hacia las granjas de servidores. La protección de dispositivos de red incluye mecanismos básicos como autenticación en routers, limitadores de tasas de transferencia para evitar que el "Control Plane" se sature, y protección ante ataques DoS/DDoS con dispositivos que filtran tráfico indeseado para evitar saturación de links. En la infraestructura de red se ajustan parámetros tales como "Control Plane Policing", limitadores de tasa de transferencia especiales para determinado propósito, autenticación de routers, seguridad en puertos además de otras características que buscan la seguridad de los puntos de acceso, como por ejemplo las VLANs (LANs virtuales).

Tendencias de Virtualización y Segmentación

La virtualización y la segmentación afectan a los entornos de los Data Centers y otros lugares en la red como los campus de WAN, oficinas regionales, y bordes de Internet. La virtualización y la segmentación proveen funciones que requieren los entornos donde tanto el control de los recursos como los dispositivos de red se hacen basados en los roles de los usuarios o sus funciones. El acceso de los usuarios se controla en los puntos de acceso y se refuerza a través de la red. Las funciones que proveen los dispositivos de red requieren instancias lógicas (virtuales) desde un solo elemento físico para permitir el uso concurrente en diferentes entornos de aplicación o en diferentes grupos de usuarios. El acceso a los datos se controla basado en los entornos de aplicación y restricciones específicas, que se refuerzan con instancias de elementos de red. En la figura 2, se muestra el tráfico de los usuarios transportado sobre caminos aislados hacia las granjas de servidores donde los firewalls virtuales, los "load balancers" (balance de carga) virtuales, entre otros, controlan el acceso a las aplicaciones, las que pueden estar corriendo en servidores virtuales. Los diferentes entornos de aplicación se segmentan usando VLANs, VSANs, y políticas en los firewalls y "load balancers" aplicados a través de instancias lógicas de servicios.

Virtualización

La tecnología de virtualización cubre un rango amplio de capacidades aplicadas a entornos de servidores y aplicaciones - desde dispositivos de red como firewalls y "load balancers", o componentes de infraestructura como routers y switches. La virtualización de servidores y aplicaciones se refiere al uso de instancias lógicas de esos recursos de forma tal que de alguna manera son independientes de la plataforma de hardware en la cual corren. Los servicios de aplicación (sistemas operativos y software de aplicación) son, esencialmente, una instancia lógica en un servidor que se mueve fácilmente hacia cualquier otro servidor cuando sea necesario. Esto requiere imágenes preexistentes del servicio de aplicación y puede requerir de la separación entre las funciones de I/O (entrada/salida) y de que la plataforma del servidor permita la fácil manipulación de las instancias lógicas.

Existen básicamente dos tipos de virtualización de servidores. En una, un solo servidor físico está dividido en muchas entidades lógicas, o servidores virtuales, cada uno corriendo su propio sistema operativo y entorno de aplicación. En el otro, múltiples servidores son agrupados lógicamente para verse como un solo servidor con un solo sistema operativo en el cual la capacidad del CPU puede incrementarse o decrementarse agregando o sacando servidores, lo que simplifica la administración de múltiples configuraciones de software o hardware.

La virtualización de servicios se aplica a grupos de multiusuarios para aislarlos unos de otros, y en entornos de aplicaciones "Multi-Tier" (de varios niveles), para aislar una capa de otra. Con un solo entorno de aplicación, cada capa tiene sus propios requerimientos de escalabilidad y seguridad, estos requerimientos se preservan a lo largo de distintos entornos de aplicación. Las funciones basadas en red aplican a cada capa y cada entorno de aplicación independientemente a través de las instancias lógicas. La capacidad de definir y aplicar instancias lógicas de funciones basadas en red se realiza a través de la función de virtualización., lo cual se denomina "contexto virtual". Un ejemplo de un con-

Mauricio Arregoces, CCIE Nro 3285, es manager de un grupo de ingeniería de CISCO orientado a diseño y arquitecturas de redes. Es Licenciado y Master en Ciencias de la Computación y ha escrito mucho material sobre networking en Data Centres.
Se lo puede contactar en marregoc@cisco.com



CISCO SYSTEMS

customer satisfaction. powered by Cisco®

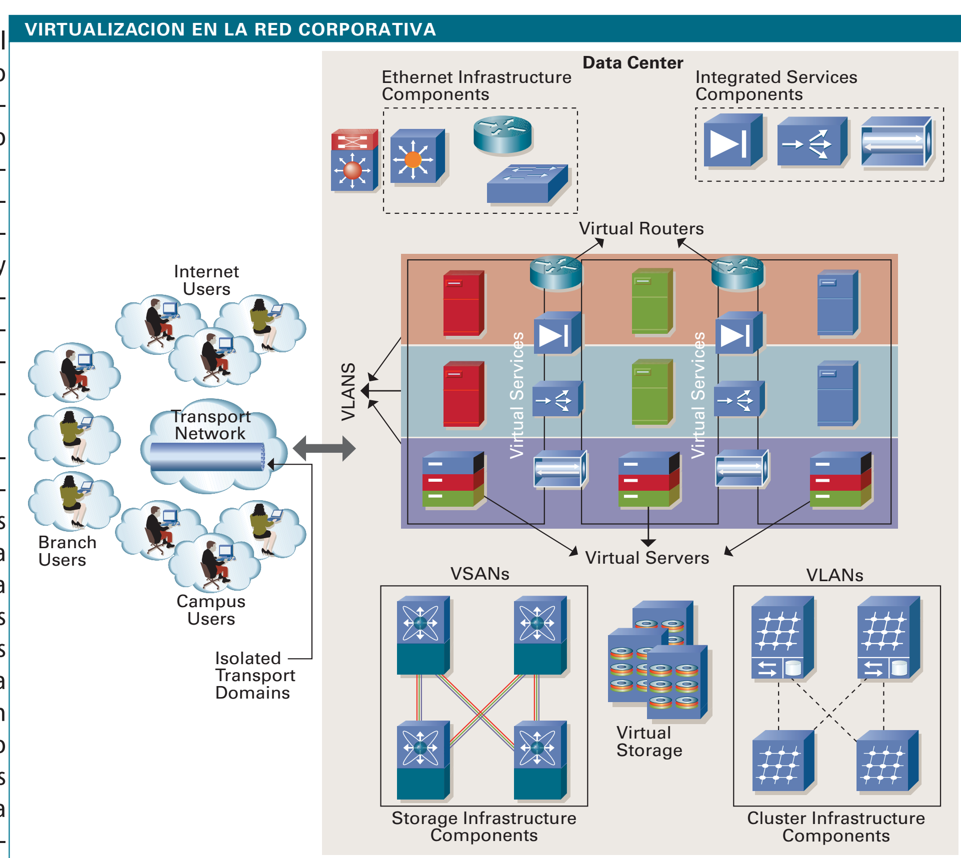


FIGURA 2
A través de la virtualización y la segmentación, es posible la creación de múltiples topologías en una única infraestructura física, optimizando así el uso de servidores y recursos de red.

texto virtual es un firewall virtual aplicado en cuatro entornos de aplicación distintos, donde cada entorno virtual se configura independientemente por entorno de aplicación. La función de firewall es virtual y la política general se centraliza mientras que las instancias específicas se administran independientemente.

La infraestructura de virtualización provee flexibilidad usando funciones como VLANs y VSANs para permitir separación lógica de los grupos de recursos de cómputo. Estos grupos se extienden a través de la topología de la red según sea necesario, preservando las uniones de grupo. Otros servicios de infraestructura virtual incluyen routers virtuales y switches. En el ruteo virtual, las instancias de ruteo en el mismo switch físico permiten que se rutee en cada entorno de aplicación independiente, y colectivamente desde la granja de servidores a la red corporativa. En switching virtual, dos switches físicos se comportan como uno solo, de esta manera se simplifica el mantenimiento del código y la administración de la configuración, pero lo más importante es que se provee redundancia física soportando "port channelling" a través de los diferentes switches físicos.

Segmentación

La segmentación es una tendencia que aplica a todas las redes, en la cual la tecnología ayuda a separar lógicamente los grupos de usuarios y su acceso a entornos de aplicación igualmente separados. Hay tres áreas para considerar cuando se diseña un entorno segmentado, como por ejemplo el control de acceso, las tecnologías para transporte seguro y segmentos de entornos de aplicación. El acceso de los usuarios (para usuarios internos y externos) está reforzado principalmente en los puntos de acceso, que son típicamente las oficinas regionales, campus, y los entornos de borde de Internet. En esos puntos de acceso los usuarios se autentican, se autorizan y una vez que están aceptados, se ubican en el grupo al que pertenecen y son controlados por la política asociada. Una vez que están en la red, el transporte que permite a los usuarios alcanzar entornos de aplicación, provee a los mismos de caminos lógicos aislados, lo cual genera el entorno segmentado.

Los caminos lógicos proveen medios seguros para el tráfico de los clientes sobre una infraestructura compartida que termina cerca del destino del tráfico. Cuando el tráfico se destina a las granjas de servidores, el control de acceso se refuerza en el punto de acceso al datacenter.

La tecnología de segmentación es muy útil para situaciones de uniones y adquisiciones de Empresas, cuando las compañías deben unir redes, comparten un espacio de Data Center y las redes de transporte entre los clientes y aplicaciones.

Una red que ofrece servicios de segmentación requiere de varias tecnologías que se utilizan a través de toda la red, algunas de las cuales se basan en las posibilidades de la virtualización. En los puntos de acceso, los mecanismos de refuerzo utilizan IEEE 802.1X y AAA o autenticación, autorización y "accounting" (monitoreo de la actividad de un usuario), para controlar los accesos de los usuarios, las asignaciones de grupos y las políticas de grupo. Como tecnologías de transporte de los clientes se usa GRE (Generic Routing Encapsulation) o los túneles L2TPv3 (Layer 2 Tunneling Protocol Versión 3), VPNs MPLS (Multiprotocol Label Switching VPNs), o ruteo/forwarding con VPNs (VRF Lite) para ofrecer transporte seguro utilizando múltiples caminos aislados a través de infraestructuras compartidas. En el Data Center, el mapeo de caminos de transporte de datos hacia los entornos de aplicación usa routers virtuales, firewalls virtuales, y cualquier otro tipo de servicio virtual predefinido.

Continuidad del Negocio

Los planes de Continuidad del Negocio se orientan a prevenir la interrupción de la operación del negocio, en muchos países mundialmente esto se traduce en regulaciones por parte del Gobierno para las diferentes industrias para prevenir situaciones problemáticas. Para lograr los niveles más altos de disponibilidad, se necesita redundancia en las instalaciones principales de los Data Centers y también en los Data Centers distribuidos. El diseño de la red debe considerar un Data Center primario resguardado y el uso de múltiples Data Centers: uno primario, uno de backup cercanos físicamente para permitir la replicación, uno remoto para replicación asincrónica, y muchos Data Centers en modo activo-activo. Las áreas tradicionales para Continuidad de Negocio por lo general tienen una extensión con una SAN y replicación de datos entre Data Centers distribuidos. Funciones adicionales incluyen la selección de instancias de aplicación más cercanas al usuario, conocidas como "Selección de Sitios", y la elección de la tecnología de transporte que soporte tráfico storage/storage, cliente/servidor y servidor/servidor. En entornos servidor/servidor el transporte puede incluir también el soporte de adyacencia en capa 2 entre los clusters de servidores, lo que se conoce como "stretched clusters" (clusters estirados).

Entorno Físico del Data Center

El entorno físico cambia como resultado de la consolidación de los Data Centers, servidores,

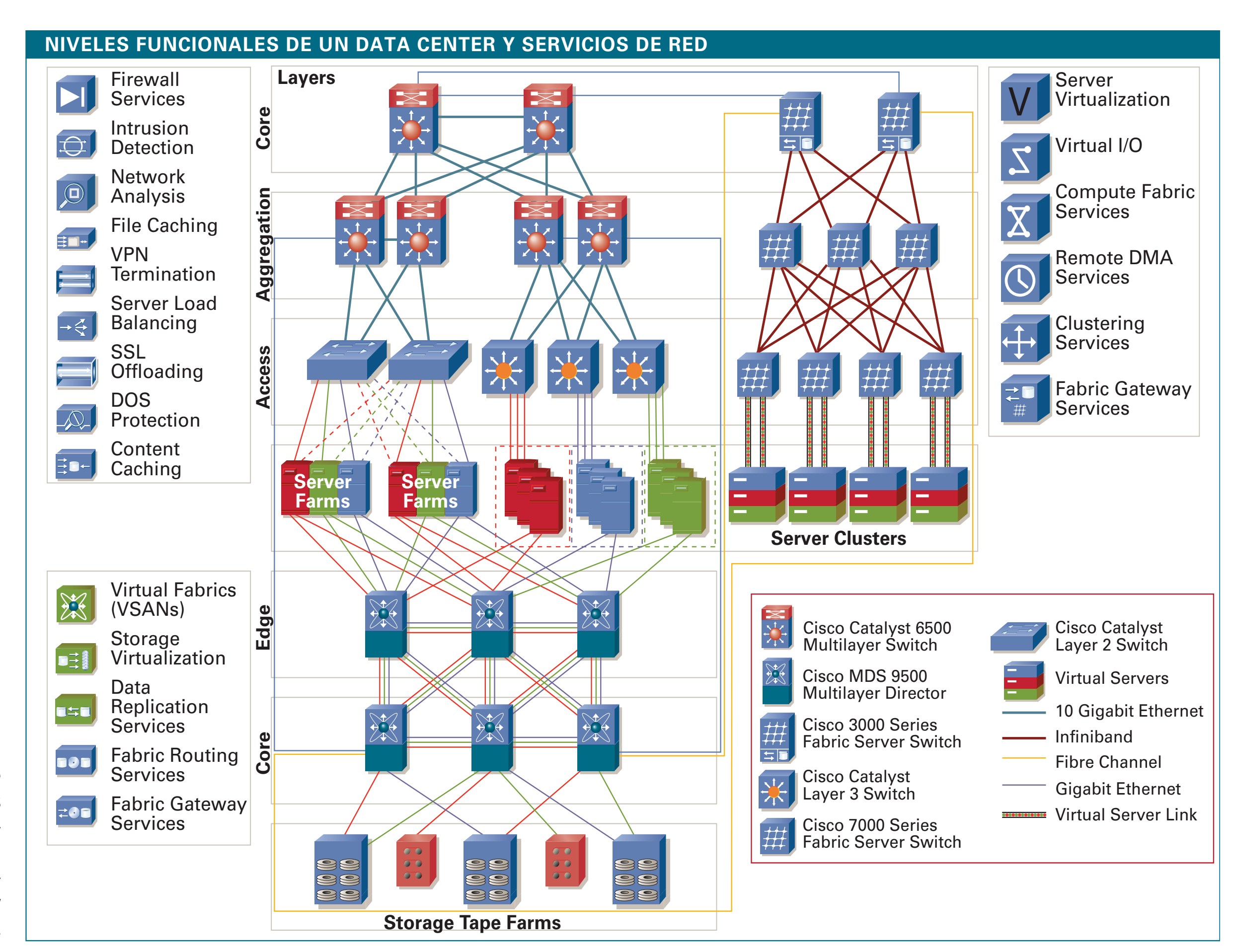


FIGURA 3
El uso de switches provee los medios físicos (Ethernet, Infiniband) y servicios para la conectividad client-to-server, server-to-server, server-to-storage y storage-to-storage.

aplicaciones, y storage; por la necesidad de proveer continuidad de negocio; y por la evolución natural de los entornos de aplicación: alta performance, mejores tiempos de respuesta, y mayor escalabilidad. Los problemas ambientales críticos incluyen alimentación, refrigeración, cableado, y espacio de piso y racks. El planeamiento de los Data Centers también incluye un crecimiento razonable de unidades de refrigeración, de alimentación y de capacidad de cómputo por unidad de rack, espacio en los racks, y hasta el número de puertos por rack.

Nueva Arquitectura de Data Centers

Las tendencias recientes presentan muchos desafíos, que tomados colectivamente, requieren del desarrollo de una red robusta que facilite la adopción de nuevas tecnologías. El siguiente criterio es muy importante para la arquitectura del Data Center: seleccionar la infraestructura de red subyacente (network fabric), determinando los servicios del Data Center, e identificar los objetivos de los entornos distribuidos.

Infraestructura Subyacente de Red del Data Center (Data Center Fabric)

La infraestructura de red del Data Center es la estructura de switches completa que soporta a las granjas de servidores (Ver la figura 3). La infraestructura de switches provee las funcionalidades claves y las posibilidades para hacer el intercambio de comunicaciones desde, hacia y entre dispositivos mucho más eficiente. El intercambio de comunicaciones cae dentro de alguno de los siguientes tipos: cliente/servidor, servidor/servidor, servidor/storage y storage/storage. El tráfico cliente/servidor pertenece a aplicaciones transaccionales donde los usuarios interactúan con las aplicaciones. El tráfico server/server es el resultado indirecto de las comunicaciones cliente/servidor (servidores de aplicación intercambiando datos de estado, servidores de aplicación intercambiando información con servidores de base de datos, y servidores de bases de datos consultándose entre sí) o la necesidad de los servidores de intercambiar información que pertenece a un solo trabajo que se dividió en tareas más pequeñas (análisis computacional). El tráfico server/storage consiste en hosts accediendo a su disco destino en un storage array o accediendo a un subsistema de cintas en un acceso por bloque tradicional. Con storage/storage, el intercambio es entre storage arrays típicamente usando un protocolo de comunicación sincrónico o asincrónico en escenarios de replicación de datos.
Las opciones de conectividad incluyen Ethernet y Fibre Channel, y las tecnologías emergentes como por ejemplo Infiniband. Ethernet continúa evolucionando, ya que ofrece mejor performance y menor costo, y redes muy probadas para entornos cliente/servidor. Fibre Channel es la opción más usada para las SANs porque provee capacidades críticas en el intercambio de comunicaciones del estilo storage/storage o server/storage.
Infiniband surge soportando un alto throughput, baja latencia, bajo costo, y capacidades críticas en entornos de clusters de servidores. Cada infraestructura de red ofrece una alternativa diferente de conectividad, y cada una provee un conjunto de servicios que soportan distintos tipos de tráfico y sus requerimientos específicos.

Servicios de Data Centers

Los servicios de Ethernet se aplican primordialmente a tráfico cliente/servidor y algunas aplicaciones de tráfico servidor/servidor. Estos servicios incluyen seguridad, optimización de las aplicaciones, y administración de la red. Los servicios de seguridad incluyen firewall, detección de intrusos, seguridad IP (IPSec), Secure Socket Layer (SSL) VPN, y servicios para evitar ataques del estilo DoS o DdoS, así como también servicios de red básicos como supresión de broadcast, inspección ARP, y PVLANs. Los servicios de optimización de aplicaciones incluyen balance de carga de servidores, SSL offloading, y dos tipos nuevos de servicios: cache de archivos y manipulación de mensajes (message manipulation). Los servicios de caché de archivos se utilizan en la consolidación de servidores permitiendo la centralización de los archivos en el Data Center mientras mantienen una performance

similar a la que tiene el usuario antes de la consolidación. Los servicios de manipulación de mensajes aplican al intercambio de información entre distintas aplicaciones y tratan de simplificar la integración de las aplicaciones empresariales.

Los servicios de administración de redes incluyen administración tradicional de elementos de red y funciones de suministro, pero las nuevas tendencias se focalizan en suministros end-to-end de servicios virtuales, incluyendo recursos de cómputo (servidores y aplicaciones) así como también redes y sus servicios. Otras funciones de redes adicionales usan capacidades de monitoreo para crear información correlativa usada para análisis de seguridad, planeamiento de capacidad ("capacity planning"), y optimización de aplicaciones.

La red de Storage provee también servicios de virtualización; las VSANs son islas separadas de SANs usando la misma red y virtualización de Storage, haciendo ver a múltiples dispositivos de Storage, como uno solo. Hay servicios adicionales que se focalizan en el mejoramiento de la replicación de datos entre storage arrays distribuidos y dispositivos de ruteo que permiten a los dispositivos de la SAN comunicarse con otros en otra SAN (por ejemplo, un subsistema de cintas utilizado para resguardar múltiples storage arrays ubicados en diferentes SANs en Data Centers distribuidos). Gracias a que la comunicación a las nubes Ethernet e IP también es necesaria, la infraestructura de red SAN también provee servicios de gateway que soportan iSCSI y FCIP.

La red Infiniband provee varios servicios para optimizar la operación de los clusters de servidores. La infraestructura de red de Infiniband permite construir server clusters de alta velocidad, baja latencia y poca "oversubscription".

Otros beneficios adicionales de Infiniband incluyen la comunicación optimizada interprocesos via Remote Direct Memory Access (RDMA) y acceso a la LAN o SAN. La red Infiniband también provee virtualización de servicios suministrando servidores sin discos (a través de servicios de booteo) usando cualquier combinación de sistemas operativos, aplicaciones y storage.

Entornos Distribuidos

Un entorno de Data Center distribuido ayuda a lograr mayor disponibilidad que los sitios únicos. En escenarios activo/activo la conectividad entre los Data Centers es crítica, por eso también se debería considerar la necesidad de servidores adyacentes en capa 2.

El criterio de diseño para Data Centers distribuidos incluye designar cuántos de ellos debe haber, cuál mantiene la instancia activa para una aplicación específica, las opciones de transporte entre ellos, y los tipos de tráfico compartido en la red de transporte. Otros factores de diseño incluyen la elección del lugar, si la infraestructura de transporte IP también se usa para replicación de datos, y la cantidad y ubicación de los accesos a Internet (en entornos distribuidos, hay múltiples puntos de acceso a Internet en los Data Centers).

LECTURA COMPLEMENTARIA

- Cisco data center design best practices:
http://www.cisco.com/go/datacenter
- Cisco Press book on data centers:
Data Center Fundamentals, by Mauricio Arregoces and Maurizio Portolani
(Cisco Press - ISBN: 1587050234)

Sheraton Libertador
Buenos Aires

9 y 10 de Noviembre de 2005

2do Congreso Nacional de Seguridad
En Sistemas Teleinformáticos y Criptografía

1er Congreso Hispano-Luso Americano
En Seguridad Informática

CONSECRI
CONSETIC

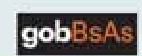
El objetivo de este evento es proporcionar un marco de discusión y soluciones, que reúna al Estado, a la Universidad, a la Empresa y a los profesionales del sector de nuestro país y del exterior comprometidos en la Seguridad Informática.

Firma Digital
Delitos Informáticos
Normas y Estándares
Aspectos Económicos
Experiencias Argentinas
Aplicaciones con Firma Digital
Registro de Poderes Revocados
Protección de Datos Personales
Normas en Tratamiento Legislativo
Auditoría de la Seguridad Informática
Investigación de los Delitos Informáticos

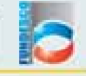
WWW.CONSECRI.COM.AR
WWW.CONSETIC.COM.AR

Auspicia:





















WorkTec

WorkTec Argentina, Teléfono: 54.11.4803.6100 o por e-mail a info@worktec.com.ar
Av. Las Heras 2925 8º Piso (1425) Capital Federal


Protegemos su mundo digital
Desde 300 metros
El Águila Calva puede divisar a su presa desde alturas superando los 300 metros, en un área de casi 5 kilómetros cuadrados.
La Heurística Avanzada de NOD32, líder de la industria, detecta hoy los virus del mañana.
NOD32 es un ganador récord de premios Virus Bulletin 100% gracias a su asombrosa detección, llevando la protección antivirus a nuevas alturas.
Tasa de detección
Fuente de información Virus Bulletin 6/2002 hasta 6/2004
Windows NT/XP
Indice de Rendimiento*
100% detectados
Eset NOD32
fallados 50
NAI Virus Scan
fallados 28
Symantec NAV
Windows es una marca registrada de Microsoft Corporation.
Symantec es una marca registrada de Symantec Corporation. Netshield es una marca registrada de Network Associaties Technology, Inc.
Bienvenidos Resellers!!
eset
www.nod32-a.com
NOD32 antivirus system

Migrando a IPv6 ya!

El futuro protocolo de comunicaciones end-to-end, puede ser fácilmente testeado hoy día.

Autor: **Leigh Huang**
Traducción: **Marcelo C. A. Romeo**

Todos los beneficios que IPv6 traerá consigo para la próxima generación de redes (autoconfiguración, direcciones ilimitadas y movilidad, entre otras) ya están al alcance de todos. Con tales características, IPv6 será sin lugar a dudas el núcleo central para una nueva generación de aplicaciones de sharing (conciertos virtuales, video meetings, juegos en tiempo real, etc.) que harán uso de sonido, video y todas aquellas capacidades multimedia que la tecnología pueda brindarnos.
Contrariamente a la falsa percepción existente en el mercado, IPv6 ha dejado de ser una tecnología distante. De hecho, ya viene soportado por varios sistemas operativos como ser Windows XP SP1 y SP2, Windows Server 2003, Windows CE, Pocket PC 2003, BSD, Solaris y Linux.
IPv6 comenzó enfrentando un típico dilema: no existiendo una demanda a nivel masivo por parte del mercado para su utilización, los desarrolladores de aplicaciones no se vieron en un principio muy entusiasmados por adoptarlo. Afortunadamente esto está cambiando, ya que tanto empresas como ISPs (Internet Service Providers) han comenzado de a poco a explorar sus beneficios, con tan sólo realizar unos pocos cambios de mínimo impacto en sus infraestructuras tecnológicas. Así, los desarrolladores ya están en condiciones de comenzar a programar aplicaciones compatibles con IPv6, con un costo y esfuerzo igualmente mínimos.

La promesa del end-to-end

Una de las dificultades clave que enfrenta el crecimiento de las aplicaciones de streaming, es la falta de conectividad end-to-end. Hoy día, Internet está basada en el protocolo IPv4, el cual no ha sufrido cambios sustanciales desde que concebido en 1981. El uso de NATs (Network Address Translators), se ha extendido como una solución relativamente útil para extender la vida de IPv4 en lo que hace al espacio de direcciones IP públicas, haciendo que compañías enteras manejen sus redes corporativas con direcciones IP privadas, saliendo a Internet con una única dirección IP pública compartida.
Sin embargo, el uso de NAT acarrea no pocos inconvenientes, ya que, desde el momento que se trata de un mecanismo de traducción, hace imposible la conectividad end-to-end entre dos máquinas que usen, por ejemplo, una aplicación P2P (peer-to-peer).



Una Internet transparente

Además de las dificultades que los desarrolladores de aplicaciones enfrentan con los entornos NAT, los administradores de red se ven obligados a implementar gateways y servidores para resolver parcialmente los problemas de conectividad. Empresas como AOL (con su servicio MegaPOP) y otros ISPs, tienen literalmente a millones de personas detrás de sus servidores Proxy; y el enrutamiento que todo este tráfico genera, consume un ancho de banda considerable.
IPv6 elimina la necesidad de NAT, otorgando a toda red conectividad end-to-end gracias a su rico esquema de direccionamiento IP. Esto hace posible que toda computadora del planeta pueda tener su propia IP pública, haciendo que las aplicaciones de networking sean más simples y rápidas, reduciendo el ancho de banda necesario y haciendo de Internet una red más transparente.
Pero, además de resolver los problemas de conectividad end-to-end y poner fin a las limitaciones de IPv4, IPv6 representa toda una oportunidad para crear un nuevo protocolo con nuevas y mejoradas características. Una arquitectura de cabecera (header) simplificada junto a una forma de operación del protocolo optimizada en gran medida, se traduce en menores costos operativos. Y con aspectos añadidos como la movilidad y la seguridad, pronto tendremos aplicaciones y servicios hasta hoy desconocidos en las redes basadas en IPv4.

Tomando impulso

Como sucede con cualquier cambio importante en el mundo de la tecnología, la migración a IPv6 se irá dando poco a poco. Ya en

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

junio de 2003, el Departamento de Defensa de los EE.UU. puso en marcha un plan para comprar el equipamiento necesario e implementar el uso de este nuevo protocolo para antes de fines del año 2007.
Por su parte, Cisco y Microsoft están seriamente comprometidos brindando el apoyo y soporte necesarios para la implementación de IPv6 en el mercado a gran escala. Ambas compañías se encuentran actualmente trabajando para organismos gubernamentales de los EE.UU., como la National IPv6 Task Force y la National Strategy to Secure Cyberspace, quienes ya están analizando posibles inconvenientes que puedan surgir durante la futura implementación del protocolo IPv6 en todo el territorio norteamericano. La industria de consumo electrónico también está demostrando compromiso al respecto. Sony Corporation ha recientemente anunciado que todos sus productos serán IPv6-compatibles para el 2006.

Microsoft y Cisco interactúan en el desarrollo de la movilidad IPv6

La movilidad IPv6 es una característica técnica diseñada para direccionar la conectividad móvil mediante dicho protocolo. Su estandarización está en manos de la Mobile IPv6 Working Group, siendo la última versión la RFC 3775. Hasta la fecha, Microsoft y Cisco ya la han implementado. Tres elementos son necesarios para lograr esta funcionalidad: el nodo móvil (mobile node) que lleva a cabo la comunicación durante el tránisto, el agente local (home agent) que eventualmente responde a las solicitudes de comunicación de los nodos móviles, y el "correspondent node" que comunica con los nodos móviles. Cisco proveerá soporte para agentes locales en routers Cisco IOS Release 12.3T. El mismo funciona también con nodos móviles que corran Windows XP SP1 y SP2, Windows CE y Pocket PC 2003.

Protagonizando la transición

Si bien la adopción masiva del protocolo IPv6 se encuentra aún algo lejana, cualquier empresa puede hoy mismo comenzar a dar los primeros pasos para familiarizarse con la implementación de este protocolo. Y gracias al soporte de compatibilidad IPv6 que muchos fabricantes están implementado últimamente en sus productos (tanto en hardware como en software), el proceso se simplifica aún más.

• 6to4 para PCs y routers que tengan al menos una dirección pública IPv4. 6to4 permite a las empresas hacer tunneling de tráfico IPv6 a través de Internet. 6to4 viene incluido en Windows Server 2003, Windows XP SP1 y SP2, como así también en el software CISCO IOS.

• Teredo para PCs y dispositivos con direcciones IP privadas, principalmente de tipo hoga-

MIGRACIÓN IPv6

Soporte para IPv6 y coexistencia con IPv4 son características que los principales fabricantes de hardware y software para redes están implementando en sus productos, incluyendo tecnologías ISATAP, Teredo y 6to4. La migración es bastante sencilla, implicando impacto y costos mínimos para la actual infraestructura de red en toda empresa.

reños. Teredo utiliza tecnología NAT, permitiendo el uso de tunneling entre dos hosts donde uno de ellos se encuentre detrás de un NAT IPv4, pudiendo ser usado también para Internet. Microsoft incluye soporte Teredo a través de su Advance Networking Pack (un free add-on para Windows XP SP1), encontrándose ya integrado en Windows XP SP2.

• ISATAP es una solución para grupos de redes de empresas, que permite el tunneling de paquetes IPv6 a través de una intranet, aún cuando la infraestructura de Layer 3 no está totalmente lista para ser utilizada bajo este nuevo protocolo. Windows .NET Server 2003, XP SP1 y SP2, y las distintas versiones de software de CISCO IOS soportan compatibilidad full con ISATAP.

Con el propósito de facilitar la conectividad IPv6 a través de Internet a los usuarios antes mencionados, varios ISPs ya están comenzando a implementar routers y relays 6to4, como así también servidores y relays Teredo en sus infraestructuras tecnológicas. Así, la transición hacia el protocolo IPv6 puede realizarse sencilla y rápidamente, implicando impacto y costos realmente mínimos.

A modo de ejemplo, un ISP sólo necesita implementar un servidor Teredo en su infraestructura de red para permitir a aquellos clientes que se encuentren detrás de un NAT, el uso de aplicaciones IPv6. Como ejemplo de aplicación IPv6 podemos mencionar 3Degrees (threedegrees.com), una aplicación peer-to-peer para file-sharing. Al momento de ser instalada en un sistema Windows XP con soporte para IPv6, dicha aplicación se configura automáticamente para hacer uso de este protocolo al ser ejecutada. Cuando dos usuarios de 3Degrees en esta misma situación logran conectarse uno a otro, la sesión peer-to-peer se establece por defecto bajo IPv6, pudiendo compartir e intercambiar todo tipo de archivos. La ventaja con respecto a IPv4, es que ahora también es posible controlar, por ejemplo, la música compartida por los usuarios en tiempo real.

ISATAP está más enfocado al ámbito corporativo. Aquellos servidores que corran Windows Server 2003, Windows XP SP1 o SP2, y cuenten con soporte ISATAP, pueden comunicarse entre ellos directamente haciendo uso de IPv6, aún cuando el resto de la infraestructura de red se encuentre trabajando bajo IPv4.

El soporte IPv6 viene ya implementado en los routers Cisco CRS-1, series 12000 y 7600, como así también en switches Layer 3, incluyendo los Catalyst en sus series 6500, 4500 y 3750.

Microsoft se encuentra actualmente trabajando conjuntamente con empresas líderes del sector, como Cisco, para continuar desarrollando, testeando y mejorando la conectividad IPv6.

Como vemos, mediante estas tecnologías de transición, las redes actuales no sufren prácticamente ningún tipo de cambios al momento de implementar IPv6. De hecho, no existe dependencia mutua alguna entre la actualización de la red y el desarrollo de aplicaciones.

Pero más allá de estas tecnologías de transición actuales, sí serán necesarias nuevas y extensas actualizaciones en la infraestructura de las redes en un futuro próximo, como ser, por ejemplo, el uso de hardware con soporte IPv6 nativo.

El soporte IPv6 nativo ofrece capacidades de networking superiores, beneficiando enormemente al usuario final y haciendo a nuestra infraestructura de red más sustentable en el largo plazo.

Desde la perspectiva del desarrollador

La facilidad con que los usuarios pueden comenzar a usar aplicaciones IPv6 basadas en las tecnologías de transición antes mencionadas, es una prueba contundente de que el mercado ya está listo para que fabricantes y desarrolladores puedan implementar este protocolo en sus productos y aplicaciones. Con la imposición y evolución del modelo peer-to-peer en Internet, y sin la necesidad de tener que volver a usar NAT, aplicaciones y dispositivos podrán comunicarse directa e individualmente unos con otros, haciendo uso de características avanzadas como la autoconfiguración y la movilidad. Esto abrirá nuevas oportunidades en el mercado, por ejemplo, de los video juegos o la telemática. Sobre todo esta última, que implica el uso de redes inalámbricas en lo que hace a la recolección y distribución de datos, crecerá enormemente.

En Japón, Matsushita Electric Works está desarrollando un sistema inteligente para control de edificios y hogares basado en IPv6. En este futuro escenario, los usuarios podrán conectar sus electrodomésticos con soporte IPv6 (heladeras, lavarropas, etc.) a una red centralizada, para administrar automática y remotamente el uso y funcionamiento de los mismos.

Con este panorama, podemos entrever que el protocolo IPv6 será implementado, en un comienzo, en las periferias de la red de redes, para luego ir extendiéndose hacia el corazón mismo de Internet. Y es justamente la combinación en el uso de las tecnologías de transición y la migración de aplicaciones con soporte IPv6, la llave que nos permitirá dar el primer paso. Y, como hemos dicho ya, de una forma rápida y sin costos hoy mismo.

Leigh Huang es IPv6 Program Manager de la división Windows Networking and Device Technology de Microsoft





+54-11 5032 7800

Web Hosting "Plan Básico"
• 150 MB Disco y 70 cuentas POP
• Servicio de Webmail
• Servidor Linux, PHP, MySql
• Panel de Control en Español
• 3 GB. de tráfico mensual

1 dominio $ 9 95 +IVA por mes



+ calidad
+ confiabilidad

www.inexar.com
ventas@inexar.com
Ventajas para Distribuidores
(Consulte costos por 10 dominios o más)

Paneles de control personalizados
Promoción por medio de banners en www.promositios.com
Aplicaciones con Base de Datos para implementar. Alta en buscadores, acceso gratuito a internet, etc.

Web Hosting Distribuidores
Plan básico en paquete de 5 dominios con las mismas prestaciones detalladas para el web hosting "Plan Básico"





J2EE-Project Experts

Snoop
CONSULTING

- Innovadores en servicios de Análisis Predictivo y Visualización de Datos.
- Primeros en mentoring en desarrollo Java-J2EE, incluyendo Frameworks Open Source.
- Únicos en Servicios de Implementación y Administración de Servidores Aplicaciones J2EE.
- Reconocidos por la utilización de Procesos y Mejores Prácticas en Gestión de Proyectos y Desarrollos J2EE.
- Líderes en implementaciones Oracle RAC sobre Linux.
- Especialistas en Web Services y Arquitecturas Orientadas a Servicios.
- Expertos en Proyectos de Desarrollo J2EE.
- Comprometidos con la mejor solución costo-beneficio para el cliente.

www.snoopconsulting.com













Organizaciones del mundo entero están volcándose a la tecnología para ser más eficientes y productivas. Las aplicaciones críticas de negocios como CRMs (Custumer Relationship Management), management de la cadena de suministros y planeamiento de recursos de empresas (ERP, Enterprise Resource Planning) están teniendo un impacto profundo, permitiendo a las compañías de todos los tamaños y formas adaptarse en tiempo real a los cambios de las condiciones del mercado, y a tener más capacidad de respuesta a las necesidades de los clientes, socios y vendedores. Sin embargo, a medida que estas aplicaciones y servicios han proliferado, la complejidad de la infraestructura y costos han aumentado exponencialmente debido a la naturaleza vertical o aislada en que típicamente lo han hecho. Muchas organizaciones hoy tienen cientos de aplicaciones separadas y bases de datos dispares con muy poca integración entre las aplicaciones. Este escenario de complejidad / costo es peor aún para los proveedores de servicios, porque muchos han desarrollado redes enteramente separadas para cada uno de los servicios que brindan.

La complejidad es el compañero constante de los profesionales de IT. Aparece en muchas formas y frentes. Está la complejidad de la seguridad a medida que las organizaciones tienen que afrontar los continuos y cada vez más avanzados ataques de los hackers, gusanos y viruses. Temas de escala (scalability). El costo siempre mayor y complicado de sistemas de integración y administración. Temas de interoperatividad de las aplicaciones. Preocupaciones de performance y confiabilidad. La lista continúa.

Estas cargas no sólo que incrementan los costos, sino que rápidamente minan la habilidad de IT de ser un socio de los negocios proactivo, encontrándose atrapado en cambio en el ciclo desalentador de tener que responder a temas de seguridad, adiciones, movimientos y cambios, degradaciones de la performance de la red y fallos de las aplicaciones.

Mientras que están desafiados a reducir gastos capitales, los profesionales de IT y redes entienden que las aplicaciones de negocios y servicios son tan efectivas como la red en la que corren. Entonces, deben seguir asegurándose que la red sea confiable, segura y accesible para aquellos que la deben utilizar sin importar su localidad. Para esto, están aumentando continuamente la funcionalidad, escala y resistencia de la red, que tiene el potencial de aumentar más aún su complejidad. Peor aún, toda esta inversión adicional no ofrece garantías de que las aplicaciones con misión-crítica y la información estén haciendo el negocio más ágil y apto para responder.

Entonces, ¿cómo reduce uno la complejidad y los costos, a la vez que optimiza el resultado de las aplicaciones y servicios que son tan importantes en una organización? Cisco cree que la respuesta está en encontrar una nueva manera de enfrentarse a como están diseñadas y construidas las redes. Una propuesta basada en sistemas (system-based) al que la compañía lo refiere como "Intelligent Networking"(haciendo redes en forma inteligente).

Intelligent Networking

Para revertir la tendencia de una customización más grande y también de los costos operacionales, hay una inclinación en la industria a implementar aplicaciones verticales hacia un acercamiento horizontal donde una red mas adaptable y rica en recursos actúa como base para un grado de integración más alto entre todos los elementos de la infraestructura.

"En el pasado, los managers de redes han seguido la estrategia de mantenerlas tan simples como fueran posibles" dice Rob Redford, vicepresidente de la sección de marketing de productos y tecnología en Cisco. "Esta estrategia era efectiva cuando los retos primarios eran la escala y el ancho de banda. Pero ahora nos enfrentamos a retos más complejos: incremento de la integración entre aplicaciones y servicios, mejorar el



Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

Una forma más inteligente de hacer redes.

Autor: **David Ball**
Traducción: **Núria Prats i Pujol**

diagnóstico de problemas y el aislamiento de fallas, y garantías a nivel de servicios y aplicaciones esenciales para empresas".

Para enfrentar estos retos, Cisco está embebiendo características de inteligencia y capacidades en la red. Pero una red inteligente también significa diseñar las redes inteligentemente, pensando primero sobre los retos de las empresas que uno quiere afrontar y después diseñar un sistema integrado que sea adaptable y lo suficientemente re-escaleable para futuras necesidades. Los tres elementos de una red inteligente son la participación activa de la red en la entrega de la aplicación o servicio, una metodología de sistemas (systems approach) al networking, con la red y el entorno computacional trabajando juntos de forma integrada, y políticas (policies) para unir a las reglas de la red objetivos y procesos de negocio.

La Metodología Inteligente

La red es el único elemento de la infraestructura que toca todos los otros elementos desde el middleware y aplicaciones, hasta servidores y usuarios finales. Es por eso, un lugar lógico donde implementar los cambios que se pueden impactar positivamente en toda la organización.

Cuando las capacidades se implementan en los puntos finales (endpoints) (PCs y servidores), los cambios deben realizarse en cada nodo distribuido o servidor, causando que la complejidad del manejo y el costo operacional crezcan exponencialmente. Pero estas capacidades pueden residir en la red, donde es más sencillo hacer cambios manejados centralmente, pueden reescalar costos de forma efectiva y simplificar las operaciones.

A través del desarrollo de estos productos así como la asociación con líderes industriales, Cisco trabaja en la identificación e implementación de estas capacidades que son más propicias para el mundo de redes, y en como éstas capacidades van a trabajar en conjunto con los otros elementos de la infraestructura en una base tipo sistemas.

"La infraestructura de red no se debe mirar más como una forma pasiva de conectividad", dice Mario Mazzola, vicepresidente senior y jefe de la oficina de desarrollo en Cisco, "sino como un participante activo e integrado en los procesos de los negocios".

Para que las redes se hagan más inteligentes, deben ser capaces de tomar decisiones en lo que respecta al manejo de aplicaciones particulares o flujo de paquetes. "La red debe mirar más profundamente en la carga de los paquetes (payload), explica Redford. "Debe mirar más allá de los encabezados (headers) de los paquetes para entender qué tipo de aplicación es, y que es lo que trata de hacer".

Esto es la evolución lógica. Los primeros routers miraban sólo los campos referidos a fuente (source) y al destino (destination) en el encabezado IP para hacer decisiones de routing. Como surgió la necesidad de decisiones más sofisticadas de routeo, Cisco sumó capacidades en software y hardware para mirar en campos de encabezado extendidos. Determinar la calidad de servicios (QoS) de modo de priorizar llamadas IP de voz, es un buen ejemplo de cómo este tipo de inteligencia es utilizada en las redes de hoy en día.

Sin embargo, los problemas de complejidad, costo, optimización de las aplicaciones no se resolverán nada más que por la inteligencia en las redes. Diferentes componentes de inteligencia deben estar presentes a nivel integrado del sistema (aplicaciones, servicios, middleware, y red), y ser controlados por las políticas de negocios que fijan la agenda para toda la infraestructura. De hecho, la inteligencia a nivel de la red no es si quiera posible sin un enfoque basado en sistemas (system-based approach) para construir los productos individuales que hacen a una solución tecnológica integrada.

La Metodolgía Tradicional

Hasta hace poco, la mayoría de los managers de infraestructura estaban focalizados primariamente en ahorrar dinero y reducir gastos primordiales. Construían infraestructuras a medida a partir de los mejores productos de la generación, tratando de reducir costos integrando componentes ellos mismos, y manejando la complejidad lo mejor que podían. Hoy, estamos pidiendo mucho mas de nuestras infraestructuras. Si seguimos con la propuesta tradicional, el tiempo y el dinero que se requerirá para integrar las infraestructuras mucho mas grandes y complejas eliminará ciertamente cualquier ahorro que se haga en el equipamiento. Productos no integrados no necesariamente se integran fácilmente si es que lo hacen. El apoyo puede ser otro problema ya que los múltiples vendors tienen que ser consultados para resolver los problemas. Por último, la gente y aplicaciones que llevan el negocio sufren a causa de estos contratiempos. Y el manager pregunta "¿Dónde esta el beneficio de la inversión que he hecho?"

"Las piezas están todas ahí, pero la metodología actual está agotada," dice Redford. "Se requieren herramientas más sofisticadas y estrategias para resolver los problemas de complejidad exponencialmente creciente".

La llave está en mirar la red y las funciones que debe hacer desde dos lados. Desde la perspectiva del sistema y la de los usuarios (end-user) lo que uno necesita que la red haga más que comenzar con cajas y unirlas a todas juntas. "Si uno se olvida de diseñar una red conectando cada componente individualmente, pero en cambio diseña un sistema de forma integrada," dice Mazzola, "uno estará construyendo una red que será completamente diferente, y tendrá capacidades mucho más grandes, con más inteligencia y poder."

Una red integrada inteligente representa un cambio conceptual en términos de cómo una red puede ser más que un centro de costos; puede convertirse en un recurso importante para ayudar a la empresa a optimizar los procesos de su negocio y alcanzar los objetivos del mismo.

Construyendo una Infraestructura Inteligente Basada en Sistemas (Systems-Based)

Actualmente, la industria de redes se ha focalizada en resolver los problemas de los clientes uno a la vez, agregando características, capacidades, e inteligencia sólo a nivel de cada producto individualmente. Como resultado, los productores de los equipamientos de redes han desarrollado componentes que tienden a incrementar la complejidad del manejo y fallan en ofrecer protección para la infraestructura existente. Teniendo cada producto individual características propias de diseño y administración, la operación, administración, y mantenimiento de una red se ha hecho más complejo y caro.

"La industria está en un punto de inflexión," explica Redford. "Los vendedores que siguen centrándose sólo en la innovación a nivel del producto van a fallar cada vez más en abastecer las necesidades de los clientes". Esto es lo que inspira a Cisco a continuar su estrategia de proveer productos innovadores, técnicamente avanzados con un diseño a nivel de sis-

temas (systems-level design).
"Todo lo que desarrollamos ahora encaja en el entorno tipo sistema (systems framework)", dice Mazzola. Cisco ha definido una serie de líneas de base (base-lines) para las arquitecturas de redes con características comunes: seguridad, alta disponibilidad, QoS (Quality of Services), multicast, virtualización, y optimización de las aplicaciones. Estas bases son, en esencia, un conjunto de estándares o especificaciones que sirven para asegurar la funcionalidad y el manejo consistente a lo largo de una amplia gama de productos que todos juntos forman las soluciones tecnológicas. "Aumentando el uso de un conjunto de características comunes y funciones de hardware, estamos haciendo productos que son más sencillos de implementar, utilizar, integrar y manejar", dice Mazzola. "Este esquema utiliza estándares abiertos ya existentes tales como XML (Extensible Markup Language), como así también nuevos estándares que serán desarrollados en conjuntos con socios y foros industriales tales como IETF". Viendo el futuro, los productos desarrollados en CISCO serán evaluados tanto por su abilidad de ser implementado y administrado como un sistema como por sus capacidades individuales. "Por ejemplo, nadie puede continuar con un desarrollo de un producto a menos que la seguridad hecha de un modo integrador y funcional sea parte del plan de desarrollo,", nos explica Mazzola.

La Seguridad - Moviéndonos Profundamente en la Red

Está ahora claro que para que la seguridad sea efectiva, debe estar presente en toda la infraestructura, y esto es por lo cual Cisco pone tanto énfasis en seguridad como uno de los requisitos base más importantes de las arquitecturas. Como se ha mencionado, la red toca cada uno de los elementos de la infraestructura; por ello, está en una posición privilegiada y única de no sólo monitorear la transferencia de información, sino además de reforzar las políticas de una forma mucha más coherente.
De hecho, es casi imposible controlar simultáneamente la condición de miles, o cientos miles, de punto extremos (end-points). Pero, la red, diseñada con las definiciones de la arquitectura e inteligencia adecuadas, puede verificar automáticamente cuándo un nuevo cliente se quiere conectar a la red para ver si el nuevo dispositivo cumple con las políticas de seguridad de la organización. A medida que la red incrementa su papel de catalizador, puede permitir un grado más grande de operatividad entre PCs, servidores y dispositivos de políticas.

Un ejemplo de esta capacidad es el Cisco Network Admission Control (NAC). La Cisco NAC utiliza la inteligencia en la red para permitir que un sistema integrado, manejado por políticas definidas por el cliente (customer-defined) pueda ser una realidad.
Cisco NAC es parte de la estrategia de seguridad de la compañía para crear redes que se auto defiendan. Funciona con software antivirus en puntos extremos como PCs o laptops para asegurase que el status de seguridad del dispositivo esté en línea con las políticas locales antes de que sea aceptada su admisión a la red. Esto se logra a través de agentes en los dispositivos, en las políticas de los servidores y en el router o switch.
"Los vendors de seguridad nos dicen que el 30 por ciento de las llamadas de sus centros de apoyo son sobre amenazas que tienen soluciones conocidas y que ya han sido solucionadas", explica Redford. "Hay un alto rango de re-infección de los gusanos y viruses porque los usuarios individuales no están siempre al día con las actualizaciones de los antivius y parches". Cisco NAC previene a los dispositivos que no cumplan con las políticas establecidas puedan entrar en la red. Dependiendo de la política especificada, si el dispositivo pidiendo entrada no ha actualizado los parches más recientes, Cisco NAC podrá poner en cuarentena al mismo, conectándolo a una subred a la cual podrá acceder solamente al servidor para bajar las actualizaciones. De esta forma, la reintroducción de virus conocidos a la red está controlada.
Cisco ha creado el programa NAC conjuntamente con compañías líderes en programas antivirus, incluyendo Network Associates, Symantec, y Trend Micro. Este tipo de colaboración entre empresas es esencial en la creación de los sistemas inteligentes e integrados, y es primordial en la visión de Cisco de la Red de Información Inteligente (Intelligent Information Network).

ASIC

ASIC (Application-Specific Integrated Circuit) es un circuito integrado (IC), customizado para un uso particular, más que desarrollado con un propósito muy general. Por ejemplo, un chip desarrollado solamente para correr un telefono celular es un ASIC. Por el contrario, un microprocesador no, porque se puede adaptar a múltiples usos.

La Red de Información Inteligente

Mientras que aspectos de redes inteligentes existen ya en muchas soluciones de Cisco hoy, la Red de Información Inteligente es la visión de construcción de redes de la compañía para los próximos tres o cinco años para ayudar a las organizaciones a optimizar los procesos de negocios resaltando la resistencia y adaptabilidad de la infraestructura, integrando nuevas tecnologías como telefonía IP y conexiones inalámbricas sin sumar complejidad, manejando los costos escalonados de sistemas de integración, e incrementando la agilidad de organización. Cisco está conduciendo esta visión para un sistema que tenga capacidades más amplias, inteligencia y poder, trabajando con líderes industriales, socios, y organismos de estándares para continuamente estrechar la distancia de la integración de la inteligencia entre la red y el entorno computacional.
En el futuro, Mazzola ve a los componentes de las redes diseñados con inteligencia para que interactúen con las aplicaciones de su negocio para realzar su performance. Por ejemplo, un ASIC en un router podrá mirar dentro de los paquetes (sus payloads) desde un sistema que da la orden. En este escenario , la red entenderá qué es lo que pasa en los Layer 4 a 7 y será capaz de entender los paquetes que llevan XML o Protocolos de acceso de objetos simple (SOAP) por ejemplo. "Si es el final del año y su servidor de transacciones ha apilado órdenes sin poderlas procesar, la red podrá inspeccionar los paquetes para ver grandes pedidos de clientes importantes con tiempos de entrega cortos ", Mazzola hacer notar.
¿Cómo será diferente el futuro respecto al presente? Una Red de Información Inteligente mirará mas profundamente el trafico de la red, no sólo en los títulos de los paquetes, sino que profundamente dentro de los payloads para hacer mejores decisiones basadas en mejor información referentes a la entrega de aplicaciones individuales. La red entregará resistencia en términos de performance a nivel de servicios, no sólo performance de la red por ejemplo, asegurándose que la información llega de la fuente a





destino, no sólo si la conexión de un punto a otro tiene un path resistente. La adminitración se hará a nivel de sistema, no sólo en una caja o elemento de base. Los recursos serán asignados y administrados dinámicamente, permitiendo ser aplicados a un requerimiento específico y luego liberado para otra tarea (esencialmente se convierten costos fijos en costos variables).

La visión de futuro empieza ahora

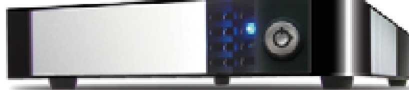
Para que la tecnología de la información pueda afrontar los objetivos de la organización, la infraestructura debe estar diseñada de forma que permita decisiones y procesos optimizados de negocios de forma que los costos se reduzcan y también la complejidad. Porque la red es la base de la infraestructura, debe ser resistente (resilient), integrada y adaptable. Esto permite a las aplicaciones, procesos, y servicios a ser más efectivos, que hacen a su vez que las organizaciones y la gente sean más productivas y provechosas.

Permitiendo inteligencia en las redes, las organizaciones tienen un mejor entendimiento de cómo operan las aplicaciones y servicios, dejando a las redes tomar mejores decisiones. Esta inteligencia no es posible sin una metodología de sistemas (sistems approach), que sea integrado y que abarque e involucre todos los aspectos de las soluciones de negocios. Aún más, los sistemas integrados ayudan a reducir la complejidad y costes proveyendo un más rápido despliegue y utilización de los servicios.

Finalmente, políticas basadas en reglas de negocios permiten a las organizaciones a adaptarse de forma única esta inteligencia a nivel de sistemas para sus propias infraestructuras. Proveyendo controles de políticas flexibles con conciencia de las aplicaciones de las redes inteligentes, los administradores de la infraestructura podrán optimizar sus redes e implementar acciones que directamente mejoren las operaciones de los negocios.

"Esta es la primera vez que Cisco ofrece esta visión del futuro", dice Mazzzola. "Pero ya estamos trabajando en el software y el hardware en implementaciones a nivel de sistema". Los elementos de redes inteligentes ya están siendo embebidos en soluciones que la compañía vende hoy. Porque la protección de inversiones es un componente principal de la propuesta de redes inteligentes, los clientes podrán adherir niveles más altos de inteligencia construyendo sobre las bases de su actual red de Cisco. Los beneficios incluyen una infraestructura segura, un despliegue más rápido de servicios y aplicaciones, reducción de complejidad, y reducción en los costos de propiedad.





Unidad Externa SohoTank
p/ discos SATA USB2.0/IEEE1394



Unidad Externa NEXSTAR 3
p/ discos IDE USB2.0
Azul / Negro / Rojo



Unidad Externa NEXSTAR 2
p/ discos IDE USB2.0/IEEE1394



Mobile Rack EZSWAP
SATA hotswap con Panel LCD



Unidad Externa NEXSTAR
p/ Disco Rígido 3.5" USB2.0



Florida 537 p.1 Local 485 C1005AAK Bs As Argentina
Te.: (011) 4393.1717 Email info@hardbug.com.ar
http://www.hardbug.com.ar



Servicios Integrados

powered by cisco

La revolución de los routers

Empresas de todas las dimensiones han comenzado a buscar un mayor grado de integración en la tecnología de redes.

Por un lado, las grandes empresas, al extenderse en numerosas sucursales, y utilizando tecnologías como VPNs (Redes Privadas Virtuales) para permitir el acceso seguro a los recursos corporativos, aplicaciones accesibles desde sitios remotos y comunicaciones de voz transportadas sobre la red de datos (VoIP), se encuentran con una red compleja, con múltiples dispositivos para los diversos servicios. Esto redunda en altos costos de mantenimiento que preocupan a los responsables de IT. La integración de servicios en una única plataforma representa para este tipo de empresas la solución necesaria para reducir agresivamente el TCO (costo total de propiedad) de la red.

Por otro lado, las pequeñas empresas también se pueden beneficiar de la integración de servicios.

Al concentrar múltiples servicios en un sólo dispositivo, no se requiere de un personal capacitado para la operación de varias plataformas de distintos proveedores, por otro lado en estos equipos se proveen herramientas gráficas que permiten de manera simple e intuitiva la operación y configuración los mismos.

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

SERVICIOS INTEGRADOS

- CONECTIVIDAD
- SEGURIDAD
  - FIREWALL
  - PREVENCIÓN CONTRA INTRUSIONES
  - IPSEC VPNs
- SERVICIOS DE VOZ
  - VOICE GATEWAY
  - IP PBX
- CONECTIVIDAD INALÁMBRICA

¿Qué desea usted de un router?

Primeramente se define al Router como el dispositivo de red que permite la interconexión de diferentes tipos de redes, por ejemplo interconecta una red empresarial con Internet, por lo tanto el router es, entre otras cosas, un dispositivo que permite la conexión hacia Internet.

La cuarta generación de routers que Cisco ha desarrollado se basa en la integración de servicios tales como seguridad, telefonía, conexión a Internet, calidad de servicio y otras funcionalidades como Wireless LAN dentro de un único equipo. Este nuevo enfoque hacia la integración responde a los requerimientos globales de las empresas, según una encuesta realizada entre cientos de empresas. En el siguiente cuadro se ilustran las funcionalidades que los clientes desean de un router:



El resultado refleja que las empresas están mayormente preocupadas por la seguridad, esto se debe a que el equipo que tradicionalmente daba la conectividad a Internet ahora además debe proteger la empresa ya que para muchos de ellos Internet dejo de ser un elemento de consulta para transformarse en una nueva forma de hacer negocios.

Las funcionalidades que tradicionalmente eran efectuadas por diversos equipos, como conexión a Internet, Firewall, conexión conmutada de PCs y servidores, conectividad inalámbrica, Central Telefónica y conexión a la red de telefonía pública, hoy pueden convivir en una sola plataforma sin verse comprometido el desempeño de la prestación de esos servicios.

La cuarta generación de routers Cisco

Los nuevos routers de servicios integrados de Cisco, por sus siglas en inglés (Cisco ISR – Integrated Services Routers), permiten a través de una arquitectura de hardware totalmente renovada, la prestación de servicios concurrentes de datos, seguridad y voz con niveles de performance hasta 7 veces superiores. Tradicionalmente, los routers sufrían en su desempeño cuando se habilitaban en forma simultánea diversos servicios demandantes de procesamiento.

Los ISRs, en cambio, gracias a nuevos componentes de hardware de aplicaciones específicas pueden realizar tareas de alta exigencia como la encriptación de tráfico, sin agotar los recursos del procesador central o CPU y a la vez realizar las tareas convencionales de ruteo, traducción de diracciónes de red (NAT) y funcionar como firewall e IPS (Sistema de Prevención de Intrusiones) entre otros servicios.

Los dispositivos que conforman esta cuarta generación de routers se agrupan en cinco familias ofreciendo distintos niveles de performance, densidad de servicios y modularidad. En la siguiente figura se pueden ver las cinco familias mencionadas posicionadas en empresas o sucursales desde 5 usuarios hasta cientos o miles de usuarios.

Oportunidad

Los ISRs han establecido una nueva evolución en la prestación de múltiples servicios y desempeño. Las empresas de todos los tamaños pueden beneficiarse de esta nueva tecnología actualizando el equipamiento de sus redes y accediendo a nuevos niveles de seguridad y funcionalidades potenciando las prestaciones de la tecnología al servicio de los negocios. ■





Un vistazo a IP Multicast

Traducción: **Marcelo C. A. Romeo**



¿Por qué debería interesarme el tema de IP Multicast?

Muchas de las aplicaciones actualmente en uso en las redes modernas, envían información de índole diversa (voz, video, datos) hacia múltiples destinos en forma simultánea. Cuando el destino de los paquetes se limita tan sólo a unas pocas estaciones de trabajo, el envío de múltiples copias de la misma información (multicast) no genera demasiados inconvenientes. Sin embargo, a medida que la red crece y las estaciones de trabajo aumentan en número, los efectos negativos del multicast comienzan a hacerse notar. La instalación masiva de aplicaciones de video streaming y comunicación por VoIP a lo largo de toda red, y sin la presencia de dispositivos apropiados para el correcto manejo de paquetes multicast, puede traer como consecuencia una severa degradación en la performance de la red.

¿Qué inconvenientes se presentan?

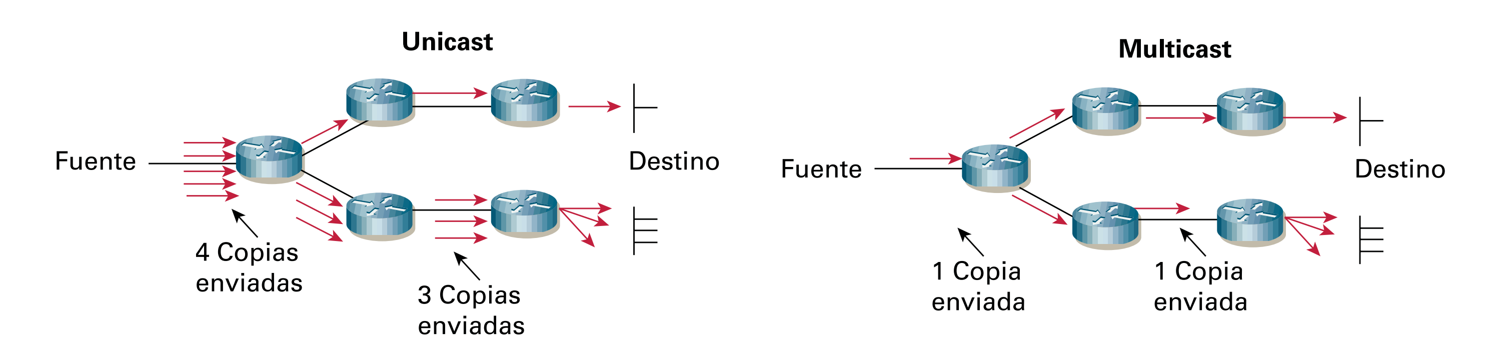
El tratamiento de paquetes multicast, requiere métodos eficientes para la distribución masiva (deployment) de aplicaciones que deban ser instaladas a gran escala por toda la red. Esto es posible gracias al uso de protocolos que reducen la congestión del tráfico de red asociada al envío de la misma información hacia múltiples destinos, aliviando las exigencias de procesamiento que sufren los routers para atender a todas y cada una de las terminales.

Internet Group Membership Protocol

Internet Group Membership Protocol (IGMP) permite a las estaciones de trabajo unirse a un grupo multicast. El unirse a un grupo multicast puede compararse con la suscripción a una sesión o servicio de uso multicast. IGMP trabaja con direcciones IP clase D para la creación de grupos multicast. Al iniciarse una sesión multicast, el host envía un mensaje IGMP a través de la red, con el objeto de determinar cuáles son las estaciones que se encuentran unidas al grupo. Luego, el mismo host envía tráfico con destino a todos los miembros del grupo multicast. Los routers están permanentemente a la "escucha" del tráfico IGMP, y envían periódicamente paquetes para determinar qué grupos están activos e inactivos. Los routers se comunican entre sí haciendo uso de uno o más protocolos, con el fin de trazar las rutas respectivas a cada grupo.

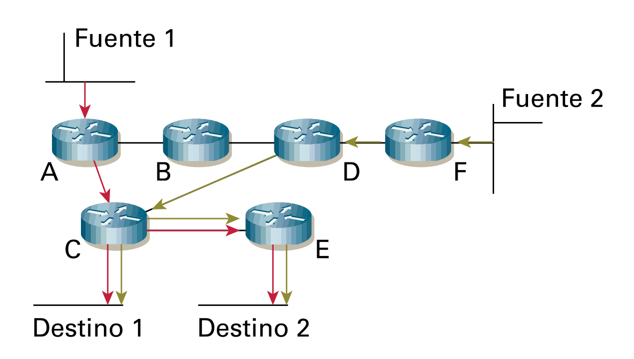
Arboles de distribución multicast

Los routers con capacidades multicast, crean árboles de distribución que controlan las rutas que todo el tráfico IP Multicast sigue a lo largo de la red para hacer entrega de los paquetes a las estaciones de trabajo destino. Los dos tipos básicos de árboles de distribución multicast, son árboles fuente (source trees) y árboles



Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

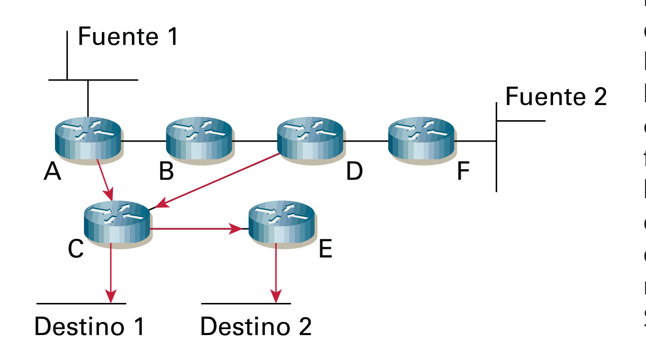
BUENOS AIRES (11) 5078-4000
LA PLATA (221) 515-4000
PILAR (2320) 65-6400
ROSARIO (341) 517-4000
CORDOBA (351) 536-4000
MENDOZA (261) 462-4000
CAMPANA (03489) 41-5010
ESCOBAR (03488) 57-5010
JOSÉ C. PAZ (02320) 60-5010
MAR DEL PLATA (0223) 411-5010
MORENO (0237) 402-5010
ZÁRATE (03487) 41-5010
BAHÍA BLANCA (0291) 496-2004
SANTA FÉ (0342) 482-8004
ENTRE RIOS (0343) 441-0004
CHACO (03722) 49-6704
CORRIENTES (03783) 41-6004
SAN MIGUEL DE TUCUMÁN (0381) 486-8004
NEUQUÉN (0299) 482-0004
SALTA (0387) 438-8004
E-MAIL: INFO@IGAV.NET - SOPORTE: (11) 4772-4706
CONECTATE 5078
USUARIO: IGAV
INTERNET GRATIS DE ALTA VELOCIDAD



compartidos (shared trees).
Mediante los árboles fuente, cada una de las fuentes envía datos hacia su respectivo destino haciendo uso de la ruta más eficiente. Los árboles fuentes están optimizados respecto de la latencia, aunque tienen requerimientos de memoria más altos, ya que deben guardar un registro de todas las fuentes.
Mediante el uso de árboles compartidos, en cambio, todo el tráfico multicast va dirigido a un punto en común de la red (conocido como rendezvous point, RP), antes de ser enviado a cada destino en particular. Los árboles compartidos requieren menos memoria por parte de los routers que los árboles fuente, pero como contrapartida puede que no siempre usen la ruta más óptima, lo que repercute en la latencia de los paquetes enviados.
Los switches Layer 2 reenvían todo el tráfico multicast, reduciendo la performance de la red. Afortunadamente existen dos métodos –Cisco Group Management Protocol (CGMP) y IGMP Snooping –, desarrollados ambos para mitigar el incorrecto funcionamiento de este tipo de switches.
Además, CGMP permite a los switches Cisco Catalyst el reenvío de paquetes del tipo Layer 2, basándose en la información IGMP. Una vez configurado en switches y routers, CGMP garantiza que todo el tráfico multicast sea reenviado sólo a aquellos puertos que corresponden a las estaciones destino. Al hacer uso de CGMP, todos aquellos routers que reciban un mensaje multicast del tipo "join" (multicast join message) procedentes de un switch, responderán al mismo con un mensaje de igual tipo. Esto es lo que permitirá tomar decisiones para el reenvío de paquetes Layer 2.
Por su parte, IGMP Snooping mejora la eficiencia permitiendo a un switch Layer 2 "ver" el tráfico Layer 3 enviado entre hosts y routers. Cuando un host IGMP envía un reporte a través de un switch, éste agrega el número de puerto del host a la tabla multicast asociada. IGMP requiere el uso de un switch para poder examinar todos los paquetes multicast, por lo que se trata una solución que sólo debe implementarse en switches de alta gama.

Multicast Forwarding

Durante el routing multicast, el tráfico es encaminado desde su origen hacia el host destino. Con el multicast forwarding, en cambio, el origen envía tráfico con destino a diversos hosts, representados por una dirección de grupo multicast. El router multicast deberá determinar la dirección del tráfico: upstream (hacia el origen) o downstream (hacia el destino). En caso de haber más de una dirección downstream, las mejores rutas elegidas para encaminar dicho tráfico pueden o no coincidir con aquellas que hubieran sido elegidas en caso de haberse tratado de tráfico unicast, proceso denominado Reverse Path Forwarding (RPF), usado para crear árboles de distribución que se reciclan libremente.



Protocol Independent Multicast

Protocol Independent Multicast (PIM) puede trabajar con cualquier protocolo de routing unicast usado para publicar las tablas de routing unicast. PIM usa la información de routing unicast para cumplir con la función de multicast forwarding, haciendo uso de la tabla de routing unicast para realizar un chequeo RPF, en lugar de tener que construir una tabla de ruteo multicast independiente. Esto trae aparejado dos tipos de comportamientos distintos, de acuerdo a la densidad o escasez del tráfico de red existente en un determinado entorno.
En el primero de los casos (PIM Dense Mode), el router multicast envía todo el tráfico hacia todos los puertos disponibles. Si el router no llegara a disponer de hosts o vecinos de downstream que sean miembros de un grupo, un mensaje del tipo "prune" es enviado hacia el router advirtiéndole de no enviar más tráfico hacia un determinado dispositivo. Este comportamiento, hace que PIM Dense Mode no sea la opción recomendada.
En el segundo caso, PIM Sparse Mode, se hace uso de un modelo explícito, donde el tráfico sólo es dirigido rumbo a aquellos hosts que han sido explícitamente especificados para recibirlo. Esto es posible gracias al envío de un mensaje del tipo "join" hacia el RP. RP unicast provee balance de carga (load balancing), redundancia y tolerancia a fallos (fault tolerance) mediante la asignación de una misma dirección IP para múltiples RPs dentro de una red de dominio multicast funcionando en PIM Sparse Mode.



zombis troyanos "bots" gusanos
¿qué hemos forjado?

Autor: **David Barry**
Traducción: **Núria Prats i Pujol**

En Junio de 2004, una gran red de computadoras zombizadas, también conocidas como robots o "bots", atacaron Google, Yahoo y otras páginas webs importantes, bloqueando el acceso a éstas por dos horas. Los expertos en seguridad fueron capaces de identificar la red de bots (botnet) y lograron apagar el ataque. Sin embargo el ataque fue sólo uno de los que USA Today recientemente describió como "ola tras ola de programas infecciosos que han saturado Internet causando que el número de PCs atacadas por hackers y convertidas en los llamados zombis haya aumentado a millones" [1].

Las computadoras zombies son las versiones técnicas de hoy en día de los cuerpos sin mentes que se levantan de las tumbas para aterrorizar a los vivos en las películas de terror de los años 60. En 2005, estos zombis operaran en el cyber-espacio proliferando a lo largo tanto de redes privadas como de Internet. Los Botnets son el mejor ejemplo del poder y complejidad de las amenazas de seguridad de hoy.

Desarrolladores sin escrúpulos crean estas amenazas utilizando gusanos, viruses o ataques embebidos en aplicaciones. Con botnets, por ejemplo, estos desarrolladores pueden usar gusanos o ataques embebidos en las aplicaciones (esto es un ataque que se esconde dentro del tráfico de una aplicación, como tráfico web o ficheros compartidos entre pares (peer to peer)), para depositar "Troyanos". Los troyanos son pequeños programas ejecutables que quedan remanentes en la computadora del usuario. Cuando un usuario confiado se conecta a Internet (y esto sucede automáticamente con cable MODEM o ADSL), los bots se conectan a un servidor para esperar órdenes de el "zombi master". De manera similar a lo que ocurrió en el incidente de Junio de 2004, los hackers pueden lanzar ataques de viruses que depositan troyanos en miles de computadoras, con pleno desconocimiento por parte de los dueños de esas computadoras. Un zombimaster puede usar estas aplicaciones para saturar un sitio web particular con paquetes de denegación de servicios distribuida (DDoS) o inmensas cantidades de spam (ver figura).

De acuerdo con reportes de amenazas en Internet recientes de Symantec, más de 30000 computadoras son reclutadas en botnets cada día.

"Los botnets ilustran como de complicado y distribuido se ha convertido el entorno de amenazas de red" dice Scott Pope, marketing manager de productos en Grupo de Seguridad Tecnológica en Cisco. "Y, desafortunadamente, la situación continúa empeorando a medida que los hackers han crecido para hacerse más sofisticados y creativos en los ataques que generan".

Esta combinación de técnicas de ataque- un virus o gusano utilizado para depositar un troyano, por ejemplo- es relativamente nuevo y se lo conoce como ataque combinado (blended atack). Un ataque combinado puede ocurrir en fases también: un ataque inicial de virus con un troyano que puede abrir un puerto no seguro la computadora, desactivar un acceso a la lista de controles (ACL), o neutralizar programas antivirus, con idea de poco después hacer un ataque mucho más devastador.

En el Reporte de Amenazas de Seguridad en Internet semi-anual, el análisis de Symantec de códigos maliciosos – gusanos, virus, troyanos, backdoors y ataques combinados- indican que malware (software especializado en producir daño) está siendo diseñado para robar datos personales, y en particular datos financieros y contraseñas. Esta tendencia del robo de datos contribuye a que todas las empresas –y particularmente bancos y compañías de e-commerce– sean mucho mas vulnerables a comprometerse.

Un panorama de seguridad en continuo desarrollo.

Cambios en las arquitecturas de las redes y las amenazas que se han desarrollado crean nuevos desafíos de seguridad. A si mismo, el concepto de perímetro de las redes está cambiando. En el pasado, los usuarios sólo podían acceder a la red a través de contados puntos de ingreso y salida – usualmente eran los que estaban conectados a Internet en la red de la empresa. Las empresas pusieron seguridad en los perímetros de Internet utilizando firewalls y sistemas de detección de intrusos (IDS).

En contraste, muchos más medios para acceder a la red existen hoy en día. El perímetro se ha extendido y distribuido, por lo que la seguridad debe ser aplicada a cada uno de estos puntos de ingresos y egresos para evitar amenazas que puedan dañar, complicando las arquitecturas de seguridad. Las redes privadas virtuales (VPNs), por ejemplo, permiten a los usuarios de las empresas usar acceso remoto a la red de la corporación y se han estado utilizando mucho más que hace unos años. Mientras que antes las empresas insistían que los programas VPN corrieran sobre una computadora específicamente configurada para la empresa, los usuarios actuales usan VPNs desde sus propias computadoras o hasta desde los locutorios u otros comercios. Este fenómeno permite muchas más entradas a la red de la compañía y presenta un desafío significativo para los departamentos de IT. ¿Está la computadora dotada de un antivirus? ¿Está el programa de protección actualizado? ¿Se ha embebido un gusano en la computadora?

LANs inalámbricas (WLANs) imponen un desafío adicional a la seguridad. Usuarios operando en una red no segura en una cafetería sin saber que puede ser que una PC "modificada", también utilizando la misma subred inalámbrica, está depositando un virus en su PC. Cuando luego esa PC se conecta a la red de la corporación, el virus puede lograr su entrada a ésta.

Al mismo tiempo, en que la red se está haciendo mas vulnerable a ataques por su gran número de puntos de ingreso y salida, las amenazas cambian. Además de los troyanos y botnets surgen nuevas amenazas. Dos de los más problemáticos son amenazas flash y gusanos auto mutantes.

Las amenazas flash se llaman de esta forma por la velocidad con que los viruses y gusanos se pueden propagar. En 1999 al virus "Melissa", uno de los primeros y más extendidos viruses en ese momento, le llevó 16 horas extenderse a nivel mundial de acuerdo con la Asociación de Redes Inc. En Enero de 2003 el virus Slammer logró infectar más del 90 por ciento de los hosts vulnerables mun-

dialmente en 10 minutos utilizando la vulnerabilidad conocida del Microsoft SQL Server. Nuevos virus en los siguientes meses y años se esperan que se extiendan más rápidamente. De acuerdo con Pope: "Puede ser que un nuevo tipo de virus infecte millones de hosts en 60 segundos. Por lo que cualquier defensa que creemos debe ser capaz de identificar la amenaza y responder mucho mas rápido que nunca antes".

La otra amenaza es el gusano auto mutante. Los gusanos de hoy en día son relativamente poco inteligentes. Están programados para seguir una serie de instrucciones, así como infiltrar una máquina a través de cierto puerto y una vez allí la ponen en peligro de alguna forma, causando un overflow del buffer y plantando un troyano. Si algo interfiere con estas instrucciones planeadas, el gusano carece de la habilidad de ajustarse y muere.

Ahora, sin embargo los desarrolladores les están sumando inteligencia y lógica a los gusanos de forma que si no logran completar su tarea específica puedan mutar y puedan perseguir otras líneas de ataque.

"El dilema de la seguridad es como la ley de Moore al revés", dice Pope. "Mientras que la Ley de Moore postula que la performance del procesador se doblará cada 18 meses mientras que los costes decaerán dramáticamente, la seguridad se mueve en dirección contraria las redes se están haciendo menos seguras mientras que el coste por defenderlas aumenta".

Este pronóstico está también confirmado por mi2g [2] una empresa de investigación en el Reino Unido que se especializa en seguridad de computadoras. Mig2 reporta que el daño económico de los ataques maliciosos a la seguridad de las redes fue de entre 157000 millones y 192000 millones de dólares a nivel mundial en 2004.

Combatiendo nuevas amenazas

El paradigma actual de la defensa de la seguridad es la de utilizar más y más de las tecnologías existentes de seguridad para cada segmento de las redes. Esto incluye firewalls y ACLs (access Control Lists) para bloquear el acceso y realizar inspecciones de aplicaciones, tecnologías de sistemas de protección contra intrusos (IPS, Intrution Protection Systems) para proveer inspecciones de tráfico muy granuladas e identificar amenazas conocidas, programas de encriptación para contrarestar sniffing, detección de anomalías para detectar gusanos o ataques DoS y programas antivirus para pelear los viruses. Muchas de las actuales tecnologías de seguridad fueron diseñadas para desarrollar funciones específicas con poco contexto de la amenaza de la red global.

Operando solas sin embargo estas tecnologías son poco efectivas para frenar nuevos ataques, así como también en las formas cambiantes con que los usuarios acceden a la red, por los gaps de seguridad que existen entre las capacidades de cada técnica.

Con el aumento de la complejidad de las amenazas, por ejemplo los ataques que usan una combinación de técnicas para interrumpir redes, las tecnologías tienen que operar de forma coordinada para parar los ataques y controlar mejor la actividad de la red y sus aplicaciones.

Desafortunadamente a lo largo de los años muchas compañías han tratado los problemas de seguridad adhiriendo agregando dispositivos y programas que resolviesen cada problema en particular. Esto ha llevado a la creación de elementos separados de protección: antivirus, firewalls, VPNs, y prevención de intrusos.

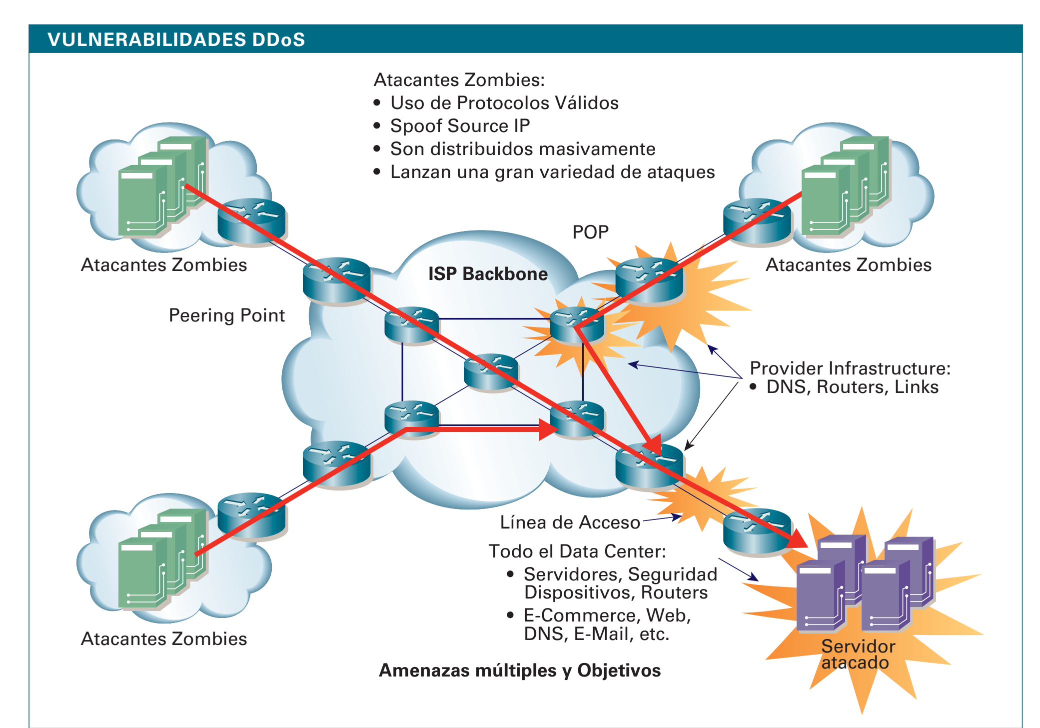
Mientras que han tratado las necesidades inmediatas, esta metodología crea un nuevo y mayor problema: manejar sistemas múltiples que operan independientemente. A medida que emergen amenazas más avanzadas, Pope y muchos otros creen que la seguridad de la red debe hacerse más integral; las tecnologías de seguridad deben actuar en coordinación para detectar y defender de las amenazas más sofisticadas.

"Hay una necesidad creciente de dispositivos que encajen las piezas del rompecabezas y tapen los agujeros que existen en los sistemas de seguridad de las redes convencionales" explica Pope. "Hay un gran problema con la clasificación equivocada de amenazas y de organizaciones tomando acciones inapropiadas, o peor aun, dejando de lado amenazas".

Seguridad adaptativa para un mundo cambiante

Transformar el caos en políticas claras y manejables es esencial, y es porqué los sistemas de seguridad de las redes necesitan centrarse en convergencia y consolidación. En seguridad en redes, un acercamiento proactivo es crítico. La idea es identificar precisamente y frenar los ataques cuanto más lejos del host como sea posible, mientras que simultáneamente se deben simplificar las arquitecturas de seguridad requeridas para hacer esto. La convergencia de numerosas funcionalidades de seguridad en un dispositivo o sistema único adaptativo permite a estas acciones conjuntas operar como una defensa coordinada (en vez de silos) que paran un amplio rango de ataques y reducen el número de dispositivos diversos que deben emplearse, y por ende simplifican el diseño de seguridad y su manejo.

Históricamente, los firewalls se han considerado generalmente objetos más o menos simples, pero son efectivos en lo que hacen: o bien bloquear un paquete o dejarlo pasar basándose en información del Layer 3 o



Ataque Zombie

Los "Botnets" son un claro ejemplo del poder y la complejidad de las amenazas a la seguridad en estos días.

Layer 4 y estados de sesión. Estos pueden proveer algún nivel de inspección de aplicaciones pero no realizan la inspección detallada de otras tecnologías. Un aparato IPS puede continuar desde el punto donde un firewall tradicional ha dejado buscando más profundamente en los contenidos de los paquetes para ver si los datos en ellos se ajustan a las políticas de la empresa. Pero a los IPS les falta amplitud de acciones para mitigar y la resistencia de los firewalls que un administrador de seguridad en redes requiere. Combinando sin embargo, un firewall con un IPS puede ser más efectivo que uno solo de ellos. Así un IPS puede pescar un ataque embebido en una aplicación que al firewall se le escape. Sin embargo el IPS quizás no tenga la acción reforzada apropiada que ofrece un firewall cuando trata con un ataque. Al converger las capacidades , los administradores de seguridad de una red tienen todas las acciones de mitigación y resistencia de un firewall con toda la inteligencia de inspección de un IPS.

Una limitación adicional de los aparatos IPS, es que a pesar de que tienen una visión detallada del tráfico de la red están basados en "firmas" (signaturas); esto significa que deben recibir updates que les digan que es lo que deben buscar. Updates de firmas pueden tardar 24 a 48 horas, haciéndolos ineficaces frente a ataques tipo flash del mañana. Allí es donde el antivirus de la red entra en juego, con sus updates dinámicos preventivos. Los antivirus se pueden poner al día muy rápidamente y pueden diseminar la información velozmente en una infraestructura a todos los puntos. Si esta infraestructura esta mezclada con IPS y un firewall, las compañías ganan más que sólo el poder de cada uno: ahora tienen un sistema de seguridad contra amenazas, así como la capacidad del firewall para bloquear paquetes que entren a la red y una solución que es altamente resistente (resilient).

Este tipo de metodología transforma el modo de enfocar la seguridad. De tener que operar como tecnologías separadas en un modo reactivo – con métodos de detección estáticos y selectivos- pasa a funcionar como un sistema de defensa proactivo que se adapta al medio de amenazas.

Según Pope, estos sistemas proveerán numerosos beneficios: detección mejorada, mayor precisión de clasificación de eventos, menores costos operativos, administración racionalizada, y extensibilidad de servicios que integran las más avanzadas tecnologías a medida que se desarrollan. Lo más importante, estos sistemas integrados no comprometerán la calidad de la seguridad en cualquier categoría, pero en cambio combinan la fuerza de cada uno de manera complementaria para entregar una defensa hermética y coordinada.

Webliografía

[1] www.usatoday.com Septiembre 8 de 2004

[2] www.mi2g.com

LECTURA COMPLEMENTARIA

- **Cisco Security and VPN information**
  http://www.cisco.com/go/security
- **Cisco Self Defending Networks**
  http://www.cisco.com/go/sdn
- **Cisco Intrution Prevention Alert Center**
  http://www.cisco.com/go/ipsalert
- **SANS Institute Internet Storm Center**
  http://www.isc.sans.org
- **eSecurity Planet Online**
  http://www.esecurityplanet.com
- **SecurityTracker**
  http://www.securitytracker.com
- **"Code that Steals for its creators"**





Panda Software se une al programa Network Admission Control (NAC) de Cisco

Panda Software tiene previsto lanzar una solución para estaciones de trabajo corporativas compatible con NAC, ClientShield con Tecnologías TruPrevent™, durante el tercer trimestre de 2005.



Panda Software anunció su incorporación al programa Network Admission Control (NAC), una iniciativa de Cisco para ayudar a cumplimiento de las políticas de seguridad informática de las empresas por parte de todos los dispositivos que tratan de acceder a los recursos de la red, de forma que se limiten los posibles daños causados por virus y otras amenazas. De esta manera, Panda Software da un paso más en su objetivo por preservar la seguridad informática de las empresas, que verá incrementadas sus opciones para defenderse de la totalidad de las amenazas de Internet utilizando las tecnologías más avanzadas. Mediante la integración de Cisco Trust Agent en las soluciones antimalware de Panda Software, los clientes comunes de ambas compañías dispondrán de una capa de protección adicional contra las amenazas de Internet. Esto se debe a que NAC verifica el nivel de seguridad de cualquier dispositivo que pueda conectarse a la red local, de forma que, si no cumplen la política de seguridad preestablecida, no podrán acceder a ella. Con ello, se evita la propagación de malware y se consigue una red corporativa más segura.

Además, la unión de Panda Software al programa NAC proporcionará otro gran beneficio a las empresas, como es la posibilidad de utilizar distintas soluciones antivirus -siempre que sean compatibles con el sistema NAC- en los diferentes equipos que se conectan habitual o esporádicamente a la red corporativa, en función de las necesidades específicas de cada uno de ellos.

El programa NAC es un componente clave en la estrategia de seguridad de Cisco denominada "The Self Defending Network", que permite a los clientes identificar, prevenir y adaptarse a las amenazas de seguridad.

"Cisco se complace de la participación de Panda Software en este programa cooperativo de la industria," afirma Russell Rice, directo de Marketing de Producto en el Grupo de Tecnología de Seguridad de Cisco Systems. Inc. "Panda ClientShield eleva el programa NAC, y ayuda a conseguir un enfoque integrado y cooperativo de la seguridad de endpoint. Esta colaboración dentro del esfuerzo de NAC, proporcionará a las organizaciones una potente gama de herramientas para ayudar a la defensa contra una gran variedad de amenazas, incluyendo ataques maliciosos, adware, intrusiones en sistemas y spyware".

Luis Corrons, director de PandaLabs, afirma: "la incorporación de nuestros productos al programa NAC de Cisco tiene como objetivo conseguir mayor seguridad y escalabilidad para nuestros clientes comunes. Uno de los más graves problemas para la seguridad de las redes empresariales es la conexión de equipos que, por alguna causa, puedan contener algún tipo de malware o estar mal protegidos, convirtiéndose en un foco de infección para el resto de equipos. "Así -añade-, "es necesario implantar estrictas políticas de seguridad que deben ser cumplidas por cualquier tipo de dispositivo que tenga acceso a la red. Nuestros productos, a los que se incorporará Cisco Trust Agent, facilitarán enormemente a los administradores la tarea de vigilancia de los niveles de seguridad de los sistemas que se conecten a la red local.

ClientShield con Tecnologías TruPrevent™, además de la más avanzada tecnología antivirus, integra sistemas de bloqueo del correo basura o "spam", así como protección contra hackers, spyware, dialers, hoaxes, jokes,...

ClientShield también permite a las empresas disponer de la protección adicional que ofrecen las Tecnologías TruPrevent™. Estas tecnologías preventivas detectan y bloquean virus desconocidos e intrusos, impidiendo la entrada y propagación de virus de como Sasser, Mydom o SQLSlammer.

Para más información sobre el programa NAC, puede consultarse la dirección: www.cisco.com/go/nac

Acerca de Panda Software

Panda Software, multinacional europea con oficinas en 50 países es una de las principales compañías mundiales de soluciones de seguridad informática. También es líder reconocido en innovación, crecimiento y en satisfacer las necesidades de los clientes con tecnologías, productos y servicios que -con el menor Coste Total de Propiedad- mantienen las instalaciones informáticas libres de virus y demás amenazas. Con las exclusivas Tecnologías TruPrevent™, las tecnologías más inteligentes contra virus desconocidos e intrusos, ofrece la mejor seguridad preventiva para todo tipo de clientes: entornos corporativos, pequeñas y medianas empresas y usuarios domésticos.

Para información adicional y copias de evaluación de todas las soluciones de Panda Software, visite nuestro sitio web: www.pandasoftware.es

Para solicitar información y asesoramiento sobre las soluciones de Panda Software contáctese con **Dast Informática**.

Distribuidor Mayorista



Dast Informática S.R.L.

Viamonte 1546 Piso 8 - C1055ABD - Bs. As. - Tel.: 011 5032-7800 - Fax (24h.365d.): 011 5258-2403
comercial@pandaantivirus.com.ar - www.pandaantivirus.com.ar

En Defensa Propia

Traducción:
Hernán D. Mazzitelli



FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

Hasta hace unos pocos años, la seguridad de las redes estaba construida sobre productos independientes ubicados en el perímetro físico de la misma, donde la LAN se unía a la WAN y las redes corporativas tenían su conectividad a Internet. El patcheado de los sistemas operativos y continuos updates de los antivirus conformaban la seguridad típica de una red corporativa.

Sin embargo, el concepto de un límite definible de la red se está evaporando. Los dispositivos del usuario a menudo se conectan con múltiples redes, transformando al perímetro en un blanco móvil. Por ejemplo las comunicaciones entre extranets de clientes y partners son hoy muy comunes. Los aumentos de la productividad producidos por las redes wireless, móviles, y los accesos remotos a la red están dando lugar a un fenómeno llamado multi-network connectivity (conectividad multi-red).

El desafío de la seguridad es que los usuarios de laptops se conectan a otras redes y a Internet desde sus hogares, hotspots públicos y habitaciones de hoteles, por ejemplo y pueden ser infectadas. Entonces, el usuario puede volver a la oficina y reconectarse directamente a la red corporativa a través de un puerto Ethernet o asociándose a un punto de acceso Wireless de la LAN pasando inadvertidamente el código maligno. Mientras tanto, es cada vez más corto el tiempo entre que ese código maligno llega a la red y se propaga a través de ella causando consecuencias muy serias. El momento en que el administrador de una red detecta un virus, gusano (worm), o Troyano (Trojan horse), u otro intruso que cause daño y logra corregir el problema, es normalmente muy tarde para que la red no caiga y se causen pér-

La seguridad de las redes basadas en el concepto de "adaptación" sigue en crecimiento: monitoreando dentro de las aplicaciones Web y suprimiendo ataques en su origen.

didas en productividad o ventas.
"Esta es la razón por la cual la seguridad ha pasado a ser un asunto estratégico de los sistemas", dice Kevin Flynn, Manager para productos de seguridad y grupo de sistemas del Grupo de Marketing de Productos y Tecnología de CISCO. "Ahora la seguridad ha llegado a ser indistinguible de las otras actividades de IT y operaciones de networking.".
Las redes se han vuelto demasiado complejas para que un solo mecanismo las mantenga seguras. Las redes modernas requieren capacidades distribuidas de seguridad, conocimiento a nivel de toda la red del contexto de las credenciales de los end-points, a medida que el comportamiento y status de los host cambian, y mecanismos de autenticación que se aseguren que se puede confiar en esas credenciales.

Protección De Cada Paquete, Cada Flujo

La estrategia de auto-defensa (Self defending Network) de Cisco, que abarca tres fases, ha estado adquiriendo rápidamente nuevos componentes para satisfacer estos requisitos. La tercera fase, llamada Adaptive Threat Defense (Defensa Capaz de Adaptarse a la Amenaza), por ejemplo, está ya implementándose, con varios anuncios de productos en marzo 2005, muchos de los cuales serán descriptos en este artículo. Adaptive Threat Defense, apunta a proteger cada paquete y cada flujo de paquetes en la red.
La primera fase de la estrategia de autodefensa de la red se basa en la integración de capacidades de seguridad directamente en elementos de la red, tales como routers, switches, puntos de acceso wireless, y dispositivos de red aislados. La segunda fase, incluye un esfuerzo de CISCO para lograr un estándar apoyado por toda la industria: NAC (Network Admission Control), implica el uso de dispositivos preparados para la seguridad (security-enabled) que se comunican el uno con el otro a modo de colaboración, tal como un sistema de prevención de intrusos (IPS) contándole a una lista de control de accesos (ACL) que niegue el acceso a una conexión. También amplía las capacidades de seguridad de los dispositivos end-point de los usuarios, que se conectan a otras redes y que podrían infectar la red corporativa.
¿Por qué se ha hecho necesaria la protección de cada paquete y el flujo? Una razón es que, cada vez más, los ataques que afectan la seguridad están siendo introducidos dentro de aplicaciones Web-enabled, que utilizan el puerto 80 de HTTP para comunicarse.
"Las aplicaciones Web, le dan poder a los usuarios pero al mismo tiempo abren puertas a abusos a través de las aplicaciones ya que el tráfico atraviesa múltiples networks y potencialmente es capaz de levantar código maligno"," dice Jayshree Ullal, Vice Presidente senior del Cisco Security Technology Group
Un gran número de productos nuevos de Cisco protegen contra el abuso de aplicaciones, identifican y frustran intrusiones en la capa 7, e incluso eliminan las fuentes de ataques. Para hacer esto, incluyen características como inspección profunda de paquetes, correlación de eventos en la red, políticas basadas en el contexto, y auditoria basada en políticas. Para combatir abuso de las aplicaciones, por ejemplo, firewalls que inspeccionan las aplicaciones han sido incluidos al dispositivo Cisco PIX 7.0 y al del software de firewall del IOS de Cisco en la revisión del programa del IOS del Cisco 12.3(14)T, así como a un nuevo dispositivo del tipo "new-generation" que combina varias de las nuevas tecnologías CISCO de seguridad: el Cisco ASA 5500 Series (Adaptative Securirty Appliance).
Los firewalls de inspección de aplicaciones ahora chequean la conformidad de puerto para HTTP (puerto 80) e E-mail (puerto 25). Es decir los motores examinan tráfico en éstos puertos de la capa 4 para cerciorarse de que es el tipo de tráfico previsto para ese puerto. "Esto ayuda a los operadores de red a controlar el mal uso de puertos por las aplicaciones tramposas que ocultan tráfico dentro de la aplicaciones Web y del E-mail para evitar la detección," dice Ullal.

Más allá del monitoreo y sistemas de respuesta de seguridad.

Un avance importante en la idea de CISCO de proteger cada paquete y cada flujo es la introducción reciente de un sistema de administración de la seguridad a nivel de toda la red llamado: Cisco Security Monitoring Analysis and Response System (CS-MARS).
"CS-MARS permite básicamente, por primera vez, un gerenciamiento completo y centralizado de una red que CISCO ha llamado CISCO Defense in Depth," dice Greg Simmons, gerente de soluciones a clientes en el Network Management Technology Group en CISCO.
El sistema, fruto de la adquisición reciente por parte de Cisco de Protego Networks, Inc.,

ESTRATEGIA DE AUTODEFENSA DE LA RED DE CISCO

FASE 1: Seguridad integrada Lanzado en el 2000	FASE 2: Seguridad de colaboración Lanzado en el 2003	FASE 3: Adaptive Threat Defense Lanzado en marzo de 2005
Las funcionalidades de seguridad están embebidas dentro de elementos de red como swiches y routers.	Las funcionalidades de seguridad embebidas están ligadas a través de la red y se extienden a los puntos finales de usuarios (user endpoints).	La red obtiene la habilidad de proteger cada paquete y cada flujo y erradicar los ataques en su origen

FIGURA 1
La seguridad es un proceso infinito, siempre en desarrollo, que abarca las tres fases de la estrategia CISCO de un "Self Defending Network".

recoge eventos de seguridad de todos los elementos de red, logs de hosts, y sesiones TCP y UDP (packet flow) en tiempo real. Los correlaciona entre ellos y con políticas de seguridad corporativas de modo de determinar si cada evento es legítimo.

"Usted podría hacer centralmente un “shut down” de una laptop que esté atacando usando CS-MARS," explica Simmons.

Todas las capacidades de seguridad integradas dentro de los routers, switches, firewalls, dispositivos CISCO y el software del IOS de Cisco -- incluyendo muchas nuevas características descritas aquí -- continúan actuando como "soldados," cada uno defendiendo contra ataques individuales sobre un end-point particular, explica Timothy Smith, ingeniero técnico de marketing del Cisco Network Management Techno-logy Group. Estos dispositivos, además de algunos otros que no son de Cisco, alimentan continuamente con información al CS-MARS.

El sistema CS-MARS, por el contrario, se comporta como el "general" supervisando completamente el campo de batalla de la seguridad. Compara información cruzada de toda la actividad de seguridad, creando e implementando toda una estrategia de combate. Todos los dispositivos en una sesión dada de TCP o de UDP entre cualquiera dos hosts, ya sean CISCO o no, reportan los datos al CS-MARS, que puede identificar cada dispositivo en la trayectoria de esa sesión.

Tener esta información permite a los encargados de red identificar un ataque, alertar al usuario, y cerrar la fuente del ataque, dice a Smith. CS-MARS enviará al administrador de la red el comando apropiado para ejecutar una acción que suprima el problema desde la red en su origen. Por el contrario, el trabajo de los soldados -- los varios productos de seguridad individuales -- es actuar sobre el efecto inmediato del ataque en su punto del impacto potencial en las varias capas de red.

Además, sabiendo la trayectoria completa que un atacante ha atravesado le permite a CS-MARS proteger la red de otras maneras. Por ejemplo, puede anticipar que la CPU o la memoria en un router dado, switch de acceso, o servidor de aplicaciones esta llegando a su limite debido a una inundación de paquetes.

"CS-MARS entonces tomaría la acción, entregando una orden, digamos, advertir a otro elemento de red en la trayectoria del dispositivo de modo de salvarlo y prevenir una denegación del servicio", por ejemplo dice Smith.

CS-MARS también sirve como un Cisco NetFlow collection engine (motor de colección). NetFlow es una funcionalidad del software IOS de Cisco para contar los paquetes en flujos de paquetes individuales, que les permite a los operadores rápidamente detectar patterns de tráfico y dar cuenta de recursos de red.“CS-MARS puede utilizar conteos de NetFlow para determinar que un puerto está experimentando un rápido incremento de tráfico, que es una variable," explica a Smith. Entonces CS-MARS determinará, basado en otros datos -- tales como firmas de protección de intrusos y registros logs de firewalls -- si un ataque está ocurriendo en un dispositivo particular; por ejemplo, en el piso 2 del edificio 6, sala de conferencias B (exhibido en la consola CS-MARS mediante estos parámetros fácilmente entendibles).

"No solamente aprendo qué dispositivos están causando el tráfico anómalo, CS-MARS me indica como apagar esos dispositivos," dice Smith.

En la línea alta, la familia CS-MARS incluye el CS-MARS 200, que procesa 10.000 eventos por segundo o 300.000 NetFlows por segundo, y en menor escala CS-MARS 20, procesa 500 acontecimientos por segundo. De un punto de vista de la configuración, CS-MARS 200 podría atender un a solo sitio grande; alternativamente, múltiples dispositivos más pequeños se podrían distribuir en los sitios alejados e informar a un regulador global CS-MARS, explica Smith.

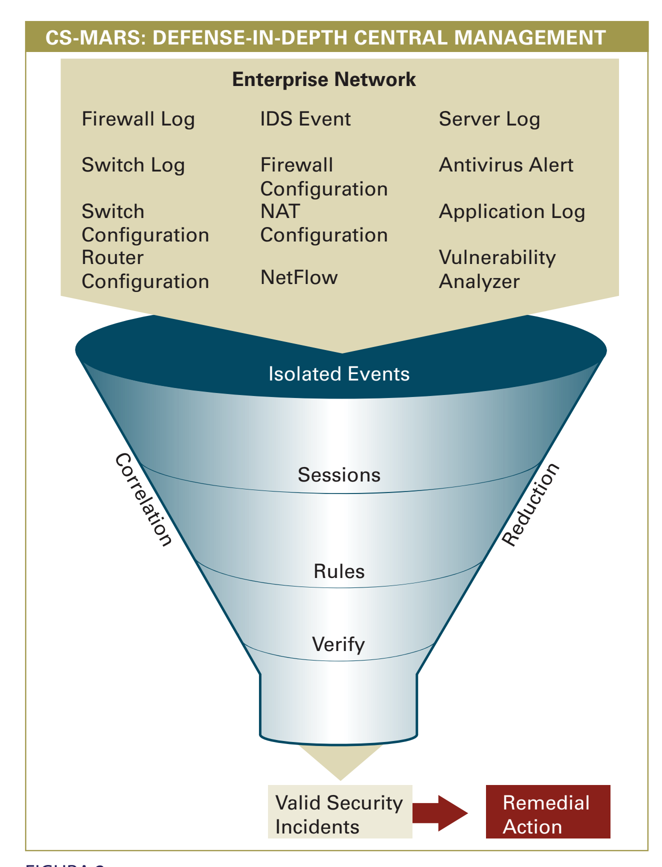


FIGURA 2

Juntando, correlacionacionando, y analizando información de seguridad que viene de dispositivos networkwide, el sistema de seguridad y gerenciamiento CS-MARS identifica y elimina fácilmente ataques de red en su origen.

Dispositivo de Seguridad Multifunción.

Un nuevo "soldado" se agrega a la lista de seguridad de Cisco, es un dispositivo integrado que se basa en la idea del Adaptive Threat Defense y que combina varias tecnologías de seguridad CISCO en un solo dispositivo extensible:

- Tecnología de Firewall
- Capacidades de VPN -- seguridad IP (IPSec) y tecnologías Secure Sockets Layer (SSL)
- Tecnología IPS (Intrution Prevention System)

La serie ASA 5500 de Cisco incluyen al Cisco ASA 5540 que es el más alto de la línea (650 Mbit/s de firewall throughput), el Cisco ASA 5520 para un funcionamiento de rango medio, y el Cisco ASA 5510 en el extremo inferior. Cada plataforma proporciona servicios de firewall a nivel de aplicaciones y la conectividad VPN flexible de IPSec y SSL. El módulo opcional Advanced Inspection and Prevention Security Services Module (AIP-SSM) soporta IPS y antivirus, worm y protección de spyware a nivel de red, según Michael Jones, encargado de línea de productos en el Cisco.

Una arquitectura única, de servicios extensibles, llamada Adaptive Identifica-tion y Mitigation (AIM), está en el corazón del diseño de la serie Cisco ASA 5500. Esta arquitectura permite que los operadores de red utilicen servicios específicos de seguridad y red basándose en el flujo de tráfico, proporcionando un control muy atomizado basado en políticas. Además, los servicios de arquitectura de AIM permiten la integración de servicios futuros de identificación de amenazas y de mitigación –lo que valoriza más la inversión y permite que las empresas defiendan sus redes contra nuevas amenazas que puedan aparecer.

Las características de la Serie Cisco ASA 5500 de poder brindar una amplia gama de roles de seguridad da costos de implementación y operación reducidos. "Por ejemplo, es posible estandarizar en este solo dispositivo muchas de las necesidades de seguridad, incluyendo firewalling, conectividad de VPN, y prevención de la intrusión," dice a Jones. Además, una interfase Web unificada para todas las funcionalidades de ASA, disminuye la complejidad de la gerencia y baja costos operacionales totales.

"Para la gente que diseña nuevas redes, los dispositivos de seguridad que buscan adaptación son una gran solución para poner todos los servicios en un solo lugar," dice a Jones, "o para remozar un sitio existente con servicios adicionales."

Cuando pienso en mi trabajo
las cosas no son como son.

Imaginar la solución a un problema y poder hacerla real. Estar en iplan significa brindar innovación tecnológica a todos los clientes.

Pablo Mosiul.
Gerente de Desarrollo de Tecnología.

TELEFONÍA + INTERNET.
Sólo iplan entendió a tiempo qué necesitaban las empresas.

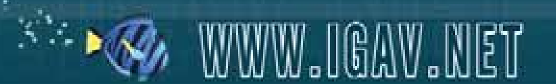
Estar comunicado significa mucho más que tener un servicio de telefonía y otro de Internet. Por eso iplan le propone que cambie. A través de un mismo proveedor para ambos servicios, su empresa podrá optimizar sus costos fijos sin descuidar la calidad. Llámenos, hay un plan para cada necesidad, sin cláusulas de salida de servicio. Desde una línea telefónica con minutos libres y acceso a Internet hasta soluciones integrales para sus telecomunicaciones.

0800-345-0112 www.iplan.com.ar ventas@iplan.com.ar



Elegí comunicarte mejor.
Elegí iplan.

Bracco, Carpintero y Nies.





CONECTATE EN BS. AS:
5078-4000

USUARIO: IGAV
CONTRASEÑA: IGAV

BUENOS AIRES (11) 5078-4000
LA PLATA (221) 515-4000
PILAR (2320) 65-6400
ROSARIO (341) 517-4000
CORDOBA (351) 536-4000
MENDOZA (261) 462-4000
CAMPANA (03489) 41-5010
ESCOBAR (03488) 57-5010
JOSÉ C. PAZ (02320) 60-5010
MAR DEL PLATA (0223) 411-5010
MERLO (0220) 402-5010
MORENO (0237) 402-5010
ZÁRATE (03487) 41-5010
BAHÍA BLANCA (0291) 496-2004
SANTA FÉ (0342) 482-8004
ENTRE RIOS (0343) 441-0004
CHACO (03722) 49-6704
CORRIENTES (03783) 41-6004
SAN MIGUEL DE TUCUMÁN (0381) 486-8004
NEUQUÉN (0299) 482-0004
SALTA (0387) 438-8004

ANTIVIRUS
MAS VELOCIDAD
ANTISPAM
CHAT
WEBMAIL
E-MAIL POP3





INTERNET GRATIS DE ALTA VELOCIDAD

E-MAIL: INFO@IGAV.NET - SOPORTE: (11) 4772-4706

CONVERGENCIA DE SERVICIOS PARA UNA PROTECCIÓN INTEGRAL

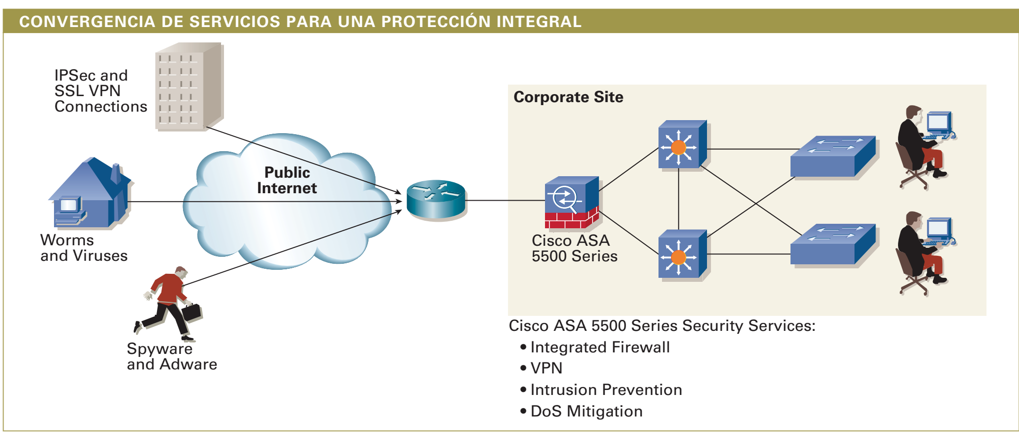


FIGURA 3

Los dispositivos CISCO ASA proveen integración de funcionalidades de seguridad que permiten diferentes políticas por-usuario basadas en credenciales IPSec o SSL.

Firewalling VRF-Aware

Según lo mencionado, el nuevo código de firewall también se incluye en la revisión IOS de Cisco 12.3(14)T. Este paso ha dado al Cisco IOS Firewall la capacidad de virtual routing y forwarding (VRF). En otras palabras, un router que está corriendo varias instancias de routing (funcionando como muchos routers dentro de un mismo chasis), puede ahora correr múltiples CISCO IOS Firewalls, explica Tom Guerrette, product manager de Cisco IOS y Router Security Marketing Group.

La nueva versión del software aplica la funcionalidad CISCO IOS Firewall a cada interfaz VRF, permitiendo que los clientes configuren firewalls por VRF. El firewall examina los paquetes IP que son enviados y recibidos dentro de un VRF. Algunas características significativas sobre el IOS firewall VRF-aware son:

-Soporta que el espacio de números IP se superpongan, permitiendo por lo tanto al tráfico de VRFs que no se intersectan tener la misma dirección IP.

-Soporta por cada VRF (y no globalmente) parámetros de comandos firewall y parámetros de Denial-of Service (DoS). En el caso de un servicio gerenciado de un service provider, por ejemplo, el firewall VRF aware puede correr como instancias múltiples asignados a varios clientes VPN.

-Se realiza la filtración del URL por-VRF.

-Los mensajes VRF-específicos del syslog que genera pueden ser vistos solamente por un VPN particular, permitiendo que los administradores de red manejen el firewall.

- Apoya la capacidad de limitar el número de las sesiones del firewall por VRF.

Las mismas funcionalidades las tiene el firewall de Cisco PIX 7.0 y también los dispositivos CISCO Adaptive Security Appliances.

Comprobación de conformidad a las políticas, las mejores prácticas

El Cisco Security Auditor es un nuevo componente de la suite de herramientas de administración de seguridad de CISCO que les permite a los clientes auditar en forma efectiva la infraestructura de seguridad de sus redes. Con la herramienta, pueden automáticamente checkear para comprobar una conformidad con las políticas de seguridad corporativa y también con mejores prácticas propuestas por la industria (como CISCO y otras) o agencias como el US Nacional Security Agency (NSA) y el Center for Internet Security (CIS).

"Teniendo la capacidad de medir, de comparar, y de hacer un report del estado de la seguridad de redes en forma dinámica, ayuda para poder manejar en forma eficiente riesgos de seguridad y conformar mandatos gubernamentales", dice Flynn.

El software permite auditar de manera automatizada miles de dispositivos, reduciendo apreciablemente el tiempo requerido en auditar una red. El Cisco Security Auditor también proporciona un modo sencillo de entender las recomendaciones de seguridad, inclusive aquellas requeridas para corregir desvíos en las políticas de seguridad, que anteriormente hubiesen requerido un análisis manual (con gran consumo de tiempo) y el uso del personal que en general es escaso.

La Iniciativa NAC de Cisco.

La iniciativa industry-wide (para toda la industria) NAC de Cisco embebe tecnología de exploración (scanning) endpoint, de partners como los desarrolladores de antivirus McAfee, Symantec y Trend Micro, directamente en elementos de red de Cisco, tales como switches, routers, y ahora, en los concentradores Cisco VPN 3000 series. Combinado con el software Cisco Trust Agent - que utiliza tecnología de autenticación de IEEE 802.1X y RADIUS – que reside en clientes endpoints de modo de mantener todas las conexiones hacia la red corporativa libre de infecciones.

Las APIs (Application Programming Interfaces) de NAC han sido abiertos a los vendors independientes de software (ISVs), que se han unido a la iniciativa de modo que las infraestructuras de redes CISCO checkeen automáticamente manejo de patches o autenticación o administración de software a través de sus propios sistemas administrativos. Entre los ISVs que venden sus productos NAC-enabled se encuentran IBM (el IBM Tivoli Security y Identity Management Product Suite); Computer Associates (eTrust AntiVirus y eTrust PestPatrol), e InfoExpress (CyberGatekeeper server 3.1 y Cyber Gatekee-per Policy Manager 3.1).

Cisco Clean Access:
NAC en forma de dispositivo.

Cisco ahora también ofrece Cisco Clean Access, la opción de un dispositivo NAC todo en uno, una resultante de la adquisición reciente de Perfigo, Inc. Debajo del paraguas de NAC, el Clean Access es una solución independiente para realizar evaluación de postura y checkeos automáticos para los más recientes updates de antiviruses y patches críticos de los Sistemas Operativos. En imple-





Soluciones open source
Consultoria especializada para empresas
Outsourcing de datacenter services
Seguridad informatica
Firewalls, IDS, Log analizers, Proxies
Alta disponibilidad y clustering
Te.: (011) 4-855-2619 informes@routix.com.ar
http://www.routix.com.ar
Routix



En Defensa Propia

mentaciones recientes del CISCO Clean Access, el número de computadoras que requirieron intervención del personal IT debido a viruses y gusanos fue reducido en forma drástica. En la Arizona State University, por ejemplo, el número de computadoras que requirieron intervención del staff se redujo de 6000 a 50 después de la implementación de Clean Access.

Clean Access no requiere la autenticación 802.1X o software cliente. Sin embargo el software cliente está disponible, y capacidades más profundas de exploración y la remediación simplificada son posibles descargando el agente, dice Irene Sandler, gerente de marketing de Clean Access de Cisco.

En el producto in-band, todos los hosts que procuran acceder a la red atraviesan el Clean Access Server. En la configuración out-of-band, que se comenzó a implementar en Abril del 2005, el Clean Access trabaja junto con los switches de Cisco para proporcionar cuarentena a las máquinas que no cumplan con los requisitos, a nivel de Layer 2 (capa 2). Estas son reparadas por el Clean Access Server. Luego de estar "reparadas" el host es puesto en la red nuevamente, "out-of-band" al Clean Access Server.

La versión out-of-band Clean Access también permite a los administradores de red crear y hacer cumplir políticas a través de un interfaz central. Las políticas se pueden definir sobre una base per-rol.

"Esto, hace extremadamente fácil que un administrador asigne cierto nivel de permisos o requerimientos de conformidad de los empleados, por ejemplo, mientras que aplica un nivel separado de la conformidad para las huéspedes," dice Sandler.

Mejoras en la Prevención De la Intrusión (Intrusión Prevention)

El IOS IPS de Cisco, presentado en la revisión del IOS de Cisco 12.3 (8) T, entrega un nuevo nivel de precisión en línea para identificar y para parar más amenazas de negocios sin la afectación de tráfico legítimo. El IOS IPS de Cisco va más allá de productos tradicionales de IPS usando análisis basados en el riesgo y la correlación en tiempo real para mejorar la precisión de la prevención, dice Guerrette. El sistema divide las firmas en signature micro engines (SMEs). En la revisión del programa del IOS del Cisco 12.3 (14) T, tres SMEs nuevos fueron agregados que representan "a donde la mayoría de los nuevos ataques parecen irse," según Guerrette. "consecuentemente, los nuevos ataques serán descubiertos y detenidos más rápidamente," él dice.

Mientras tanto, Cisco Security Agent Version 4.5 (el host-based IPS) agrega compatibilidad con los sistemas operativos fuera de los E.E.U.U. y amplía el soporte de la plataforma para incluir los servidores y desktops Linux de RedHat, y los clusters de Windows. La administración para las empresas grandes se ha aumentado a 100.000 agentes usando un solo Cisco Security Agent Manage-ment Center. La integración avanzada con NAC permite que las políticas sean dinámicamente cambiadas basadas en la postura de seguridad de NAC, el usuario registrado, o la localización del dispositivo final.

Seguridad Del Siglo 21

Con el agregado de la fase Cisco Adaptive Threat Defense a la estrategia redes de autodefensivas (Self Defending Networks), múltiples capas de seguridad han sido incorporadas que van desde un puerto ethernet al interior de las aplicaciones Web. Con esta fase se ha creado un paradigma muy mejorado de la seguridad para el siglo XXI.

La protección no depende del software antivirus y firmas," dice Ullal. "Se construye mediante conductas y clientes confiables que trabajan en forma cercana y en colaboración con la red."

Con la desaparición de un perímetro definible de la red y de las amenazas de seguridad que vienen a las redes de todos los ángulos, productos situados en un punto solamente no son más una defensa adecuada. Un sistema de varias capas integrado y proactivo hace posible la "Self Defending Network", siendo hoy un requisito para resguardar las consecuencias de los ataques de rápida-propagación -. La seguridad será un proceso continuo que estará siempre en constante evolución ya que las redes, las aplicaciones, y las amenazas serán también siempre cambiantes.

LECTURA COMPLEMENTARIA

- **Cisco Security Product Rederence Sheet:** http://www.cisco.com/packet/172_6a1
- **Cisco Self Defending Network:** http://www.cisco.com/go/security

Calidad y Seriedad en Servicios

www.sitioshispanos.com

Tu Sitio en Internet



$12,80

Alojamiento Web

Activación gratis
Estadísticas On-Line
Casillas pop3 de e-mail
Panel de control propio
Bases de datos
Registro de dominios
Asistencia técnica las 24hs.
Webmail
Backups diarios



Conectate llamando a los siguientes números telefónicos*:

AMBA (11) 5078-4004
LA PLATA (221) 515-4004
PILAR (2320) 65-6444
ROSARIO (341) 517-4004
CORDOBA (351) 536-4004
MENDOZA (261) 462-4004

Usuario: sitioshispanos Contraseña: sitioshispanos

*Consutá en nuestro sitio por números telefónicos disponibles para otras localidades.



Urquiza 1357 PA - Rosario - Argentina 0341 - 4245171

Impulsamos tu Exito



En un entorno de IT tan rápidamente cambiante como el actual las empresas necesitan capacitarse, mediante un proceso de aprendizaje intensivo y extremadamente exigente, el cual permita adquirir todos los conocimientos necesarios para la más alta administración e ingeniería y estar plenamente preparados para aplicar, desarrollar o implementar exitosas soluciones bajo las tecnologías más utilizadas.

Con currículas eminentemente prácticas, la metodología de los laboratorios permite poner al alumno en situaciones reales en el entorno de IT de una empresa.

Un claustro de profesores en permanente contacto con la realidad IT empresarial, con amplia experiencia en la docencia y en consultoría, que permite al alumno conocer de primera mano la realidad de las tecnologías estudiadas.

Continua innovación, aulas que cuentan con infraestructura y tecnología de última generación, y currículas actualizadas que reflejan los nuevos avances y versiones de las plataformas y programas de IT existentes.







Av. Corrientes 531 - Primer Piso - C1043AAF - Capital Federal -
Tel./Fax.: (011) 5031-2233 - masinfo@centraltech.com.ar -
www.centraltech.com.ar

Carreras y Certificaciones en CentralTECH:

Las carreras y certificaciones dictadas en **CentralTECH** aportan los conocimientos y la competencia de los profesionales en el manejo de productos IT. Si representa a un negocio que busca líderes en tecnología o es un profesional de la tecnología de la información, encontrará dentro de nuestro Plan de Carreras la capacitación en las últimas tecnologías.

Plan de Carreras CentralTECH:



CISSP (Certified Information Systems Security Professional) diseñada para capacitar a los profesionales de IT de su empresa con el alto grado de profesionalismo necesario en el area de Seguridad Informática.



MCP (Microsoft Certified Professional) es la certificación básica para los profesionales Microsoft. Ud. puede ser Microsoft Certified Professional y elegir su orientación, rindiendo satisfactoriamente un sólo examen.



MCSA (Microsoft Certified Systems Administrator) es la certificación para administradores de redes y entornos de sistemas basados en plataformas Microsoft Windows. Las especializaciones incluyen MCSA Messaging y MCSA Security.



MCSE (Microsoft Certified Systems Engineer) es la certificación para aquellos profesionales que diseñan e implementan soluciones de infraestructura basadas en plataformas Windows y software de servidores Microsoft. Especialización en Messaging y/o Security.



MCAD (Microsoft Certified Application Developer) está orientada a profesionales que utilizan tecnologías Microsoft para desarrollar y mantener aplicaciones de alto nivel, componentes, clientes WEB o de escritorio y servicios de datos back-end.



MCSD (Microsoft Certified Solution Developer) es la certificación idónea para profesionales que diseñan y desarrollan las últimas soluciones empresariales con herramientas de desarrollo, tecnologías y plataformas de Microsoft y con arquitectura Microsoft Windows.



MCDBA (Microsoft Certified Database Administrator) es la certificación premier para profesionales que implementan y administran bases de datos en Microsoft SQL Server 2000 sobre plataformas Microsoft Windows Server 2003.



MCT (Microsoft Certified Trainer) lo certifica como experto en formación de tecnologías, productos y soluciones Microsoft. Los Partners de Learning Solutions utilizan MCTs a la hora de ofrecer formación en Carreras Microsoft.



LINUX COMPLETA Orientada para aquellos que estén interesados en incursionar en los conceptos básicos del sistema operativo Linux: Operador, Administrador e introducción a manejo de redes Linux.



LINUX AVANZADA Dirigida a aquellas personas que deseen incrementar los conocimientos del sistema operativo Linux incorporando conceptos tales como: Curso de Redes Avanzado y de Seguridad y Contra-Seguridad de un Sistema Operativo Linux.



LINUX EXPERT Permite la especialización del profesional en un área específica por medio de la realización de distintos workshops sobre temas puntuales, tales como: VPNs, Squid, Firewalls, PHP, Servidores.

Introducción a la red SAN

¿Qué es una red SAN?

El crecimiento exponencial de la información almacenada en los centros de procesamientos de las empresas, generada por la aceleración de la Informatización y la evolución de las comunicaciones, ha llevado a la industria a crear soluciones más eficientes para la administración del almacenamiento de los datos.

Existen diversos estudios que demuestran que el costo de propiedad de una solución de almacenamiento basada en SAN (Storage Area Network) es mucho menor que tener unidades de discos directamente conectadas y dedicadas a un único procesador.

Una red de almacenamiento SAN permite que los servidores de las aplicaciones de red y de bases de datos puedan compartir recursos de equipos sofisticados de almacenamiento.

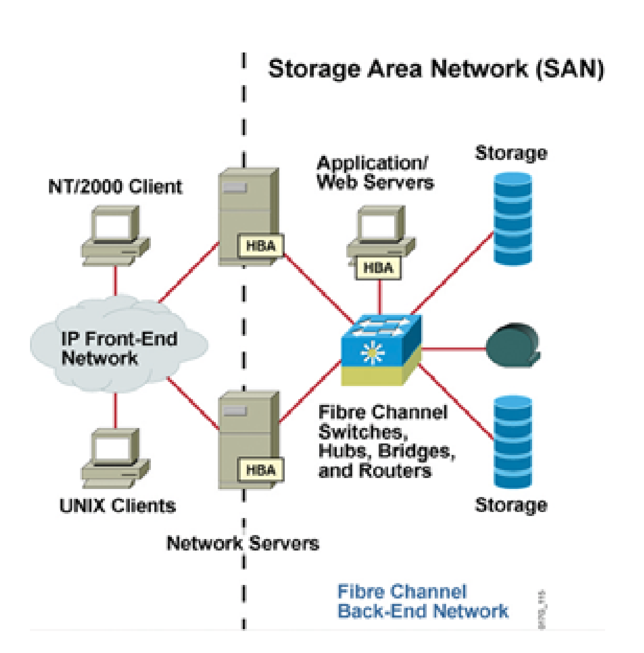
Una red SAN ofrece ventajas a los responsables de TI tales como: facilitar tareas de resguardo (procesos de Backup), facilitar la implementación de centros de recupero, realizar ampliaciones de discos con mayor tiempo de disponibilidad, aumentar la eficiencia de la capacidad almacenada, mover y compartir información entre los distintos sistemas.

¿Qué es Fibre Channel?

Una red de Storage Area Network SAN se implementa con switches de red de tecnología Fibre Channel, que permiten vincular sistemas de almacenamiento, equipos de cintas y servidores a través de fibra óptica con velocidades de 1, 2 y 4 Gbps. Fibre Channel es un estándar que está diseñando para mover grandes bloques de información a alta velocidad y baja latencia, que son condiciones requeridas especialmente en procesos de lecturas y escrituras de los servidores de bases de datos sobre sus unidades de discos.

El costo de conectar un servidor a una red SAN está en un rango de U$S 3.000 y U$S 5.000 por servidor, incluyendo la placa del servidor Fibre Channel (HBA) y precio por puerto de SAN promedio.

Debido a que el costo de conectar un servidor a la red es SAN es comparativo al costo de un servidor medio, esta solución está restringida a equipos de alta gama y aplicaciones de bases de datos críticas.



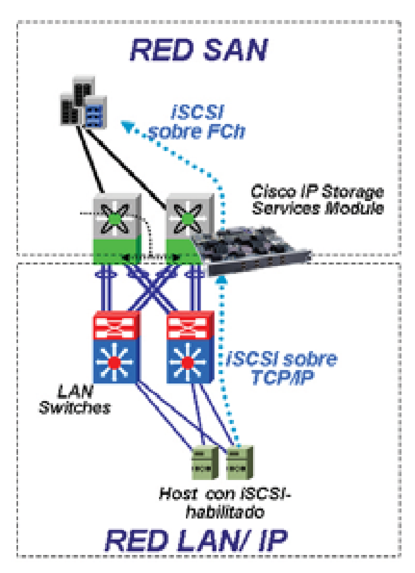
¿Cómo expandir la consolidación del almacenamiento y reducir el costo de conexión de la red SAN?

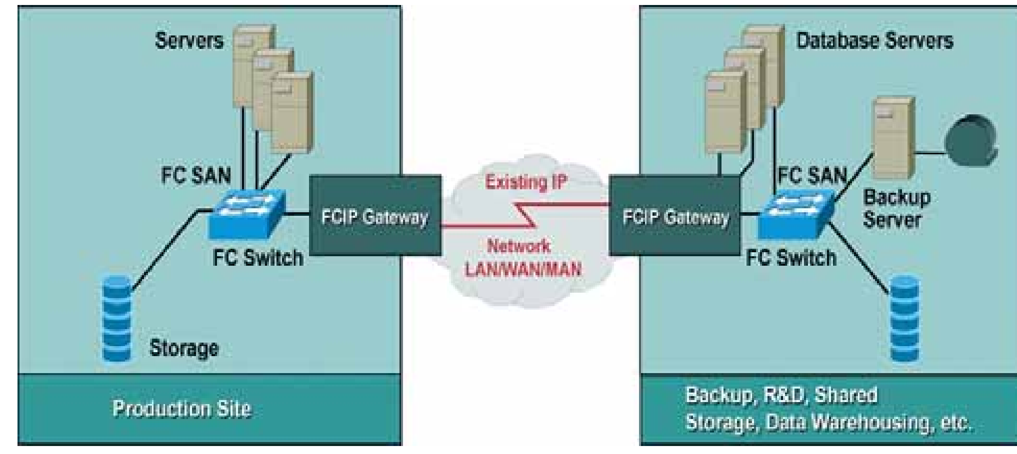
Existe la posibilidad para servidores de rango medio, de utilizar la misma tarjeta de red LAN (Gigabit ethernet /Fast ethernet) para conectarse a la red SAN.

Para ello se requiere que en estos servidores tengan instalado en el sistema operativo un driver iSCSI (iSCSI : estándar SCSI sobre IP) y que la red SAN cuente con un gateway iSCSI

FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

que vincule la red Fibre Channel con la red IP/ethernet.
Mediante la función de gateway iSCSI , la información de los sistemas de almacenamiento Fibre Channel, será vinculada a los servidores conectados a la red LAN/IP.
Con iSCSI se reduce drásticamente el costo de conexión a la red SAN, ya que los servidores no requieren tener una tarjeta especial de red Fibre Channel (HBA) ni una puerta Fibre Channel en el switch de la SAN dedicada al servidor.





¿Cómo vincular redes SAN del Centro de Procesamiento Principal con el Centro de Recupero?

La inteligencia de los sistemas de almacenamiento que se conectan en la red SAN permite mover, copiar o replicar en forma instantánea los datos entre sistemas de almacenamiento, sin la intervención de los servidores.
Muchas empresas cuyos sistemas de información son críticos para la operación de sus negocios cuentan o están planificando implementar Centros de Procesamientos Alternativos ya sean propios o tercerizados, que permita mantener sus operaciones si el Centro de Procesamiento Principal sale de servicio.
Para que esto sea posible la información almacenada en el Centro Principal, debe ser de alguna manera copiada en forma periódica o replicada instante a instante y para ello se hace imprescindible interconectar las redes SAN Fibre Channel de ambos sitios.
La opción ideal para una interconexión de redes Fibre Channel es contar con una fibra óptica dedicada y que los Switches tengan la tecnología óptica adecuada para largas distancias, que admiten una mayor atenuación de fibra en la interconexión.
El uso de la fibra óptica no siempre es una solución viable ya sea por el costo o bien por que no existe la fibra como tal.
Una alternativa de vinculación de redes SAN es por medio de una red IP de alta velocidad y usar en ambos centros equipos de red que soporten el estándar FCIP (Fibre Channel Sobre IP).
En ambas redes SAN habrá un dispositivo que tendrá una puerta de red Fibre Channel para vincularse a la SAN local y una puerta IP a través del cual establecerá una conexión FCIP con el equipo remoto.
La solución FCIP agrega mayor latencia que una solución óptica pura y por ende se recomienda su uso para copia o replicación asincrónica. En el caso que se requiera replicación sincrónica deberá evaluarse una solución óptica pura.
Cisco Systems tiene soluciones de redes SAN que cuentan con importantes avances y ventajas, entre las cuales podemos mencionar la posibilidad de integrar soluciones Fibre Channel y funciones de iSCSI gateway y FCIP en un mismo chasis, sin necesidad de incorporar equipos adicionales.
Además Cisco ha sido el creador del concepto de VSAN, que permite crear dominios Fibre Channels independientes en una misma infraestructura de red. A través de VSANs una empresa puede mantener la separación de sistemas de almacenamientos dedicados para ciertos ambientes informáticos, sin tener que aprovisionarse de switches Fibre Channels aislados. El uso de las VSAN mejora la estabilidad y escalabilidad del sistema y disminuye la complejidad y el costo de propiedad de la solución de almacenamiento.



Gabriel Sakata
Systems Engineer Manager
de Cisco Systems



Propiedad intelectual y modelo de negocios

En esta lucha casi sin cuartel entre el software open source y el propietario (o privativo, como les gusta decir a la gente del software libre), se intercambian conceptos, las más de las veces, con intencionalidad… cómo decirlo… política, en el mejor de los casos. Lo que está en juego en realidad, son los modelos de negocios, basados uno en la "protección" de la propiedad intelectual (venta de licencias), el otro en los servicios asociados a un producto libre o de código abierto.



Ricardo D. Goldberger
Periodista científico especializado en Informática y Nuevas Tecnologías. Produce el newsletter electrónico T-knos, conduce "El Explorador Federal" por AM Radio El Mundo y colabora en Gillespi Hotel, en FM Rock & Pop.

Las empresas que basan su modelo de negocios en el software propietario no pierden ocasión de argumentar contra el open source, basados, algunas veces, en las debilidades (que las tiene) del soft de código abierto, y también en mitos, varios de los cuales el tiempo se ha encargado de abolir. Por el contrario, los partidarios del software libre aprovechan cada canal de comunicación que se les ponga por delante para denostar al propietario (comenzando por llamarlo privativo, porque priva de la libertad que el software libre cree que hay que tener respecto del código) y basan muchos de sus argumentos en la mala utilización de la (para ellos mal llamada) propiedad intelectual o, más precisamente, de las regulaciones que protegen los inventos (patentes) y las obras intelectuales (derechos de autor o copyright). En general propenden a su abolición.

La mayor parte de las empresas basadas en la venta de licencias de uso (algo que puede fácilmente asimilarse al mover cajas de cualquier otro producto) como Microsoft, Symantec o Computer Associates (sólo por nombrar algunas como ejemplo) han incursionado, con mayor o menor timidez, en la oferta de servicios, pero no logran olvidar su pasado de vendedores de licencias e intentan ganar dinero por los dos lados: por la venta de las licencias y por los servicios.

Por el otro, las empresas basadas en código abierto (lo que también es, en definitiva una forma de propiedad intelectual, ya que las licencias como GPL y similares no hacen otra cosa más que proteger el derecho del autor del software) toman el software como un commodity, algo que viene "incluido en el paquete" y ofrecen (y cobran) por los servicios asociados.

No vamos a entrar en el tema de los distintos modelos de desarrollo (catedral y bazar, como los definió Raymond) pero sí a hablar un poco del tema de la propiedad intelectual, sobre los mitos y leyendas que rodean al tema.

Como primera medida, digamos que las regulaciones que se refieren a la propiedad intelectual (llamadas patentes, copyright, derecho de autor o como se prefiera) lo que tratan de hacer es de mediar entre el interés del autor de un contenido de lucrar con él y el de la población de acceder a ese contenido. Es por eso que la mayor parte de las leyes (por no decir todas) conceden al autor el monopolio de uso del producto por un tiempo limitado, después del cual éste queda a disposición del público.

De más está decir que el tiempo y los intereses han distorsionado grandemente este tipo de derechos, como por ejemplo, conceder derecho de uso por muchos más años que la vigencia del producto o restringir tanto el acceso del público que el monopolio se vuelve virtualmente permanente. Una reacción a estas tergiversaciones del deseo original del legislador ha sido, entre otras, la aparición de los movimientos alrededor del software libre o en contra de la aplicación de patentes al software.

En respuesta a estas reacciones, los defensores del derecho de autor tal como está en este momento, difunden una serie de argumentos para defender esos derecho, muchos de los cuales tienen más de mito que de realidad. Veamos algunos de ellos a la luz de la historia.

• Sin protección de la propiedad intelectual, nadie produciría trabajos originales. Como la primera ley de propiedad intelectual es de 1623, podríamos pensar que nadie hizo trabajos originales antes de ese año.

• Aún si la gente creara trabajos sin protección de la propiedad intelectual, la calidad de esos trabajos sería baja. No creo que Shakespeare cuando escribió Julio César, ni Cervantes cuando creó su Quijote, ni Haendel cuando compuso su Oratorio El Mesías se hayan preocupado por la protección de su propiedad intelectual. No creo que Leonardo Da Vinci haya creído que hay que proteger La Última Cena, por lo menos no de Dan Brown. Y así podemos seguir mencionando a Rafael, Platón, Lope de Vega, Chaucer y tantos otros que crearon maravillas sin propiedad intelectual.

• Eliminar la propiedad intelectual significa negar a los creadores el derecho de lucrar con su trabajo. Este mito está basado en la idea de que la única manera de hacer dinero es vender la idea que se produce. O sea, consultoría, soporte, servicios, afinación, no producen dinero proveniente de esa idea.

Estos y otros conceptos más (como que la propiedad intelectual es un principio antiquísimo, siendo que la primera ley de patentes se promulgó en 1623 y la primera ley considerada precursora del copyright es de 1710; o que la propiedad intelectual es un principio aceptado universalmente) se usan como argumentos en contra de los que piden un cambio o la abolición de los derechos de autor.

Es muy posible, además, que para el software, haya que pensar en algún régimen particular, ya que, a diferencia de lo físico, es posible que dos o más personas obtengan el objeto simultáneamente o, en otro caso, ¿cómo diferenciar un original de una copia, cuando una copia digital es exacta al original que, por otra parte, es un intangible del que sólo se vuelve real el soporte? Es posible que hayan intereses muy poderosos detrás de un status quo de no innovar en materia de propiedad intelectual. Pero tarde o temprano deberán hacerlo.

Nota: Esta columna se basó en el documento Some myths about intellectual property que está publicado en : http://www.ifla.org/documents/infopol/copyright/ipmyths.htm, en el sitio de The International Federation of Library Associations and Institutions.

Advanced Security Enterprise





for Microsoft
Products & Platforms



Security Solutions

www.secure105.com.ar / (54) 11 5031-2288



UNIX 100

:: **Recursos**

- 100 megabytes en disco.
- 20 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 2 Gb de transferencia mensual.
- 1 Redireccionamiento
- 1 cuenta FTP, SSH.

14.95



UNIX 700

:: **Recursos**

- 700 megabytes en disco.
- 200 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 10 Gb de transferencia mensual.
- Redireccionamientos ilimitados.
- 25 cuentas FTP, SSH.

24.00



NT 100

:: **Recursos**

- 100 megabytes en disco.
- 20 cuentas de email pop3.
- Alias ilimitados.
- Autoresponders ilimitados.
- Panel de Control Personal 2.1!
- Cgi-bins, Perl y Java scripts.
- 2 Gb de transferencia mensual.
- 1 Redireccionamiento.
- 1 cuenta FTP.

24.95

towebs®
Webhosting

Tome el control de su Website

Por que elegirnos:

:: Atención online y telefónico las 24hs.
:: Datacenter propio.
:: Más de 10.000 websites confían en nosotros.
:: Exclusivo sistema de chat online.



Tel: +54 (11) 5031-1111

Av. Belgrano 1586, piso 10 - info@towebs.com - http://www.towebs.com

CISCO SYSTEMS

FuentesdeConsulta

La información sobre los productos, las tecnologías y las soluciones de redes Cisco se encuentra disponible en diversas fuentes impresas y en Internet:

- Cisco Marketplace
Ofrece una gran variedad de libros, guías de referencia y productos Cisco.
http://www.cisco.com/go/marketplace/

- Cisco Press
Edita una amplia gama de publicaciones de ámbito general sobre redes, formación y certificaciones Cisco. Los usuarios noveles y los expertos podrán aprovechar estas publicaciones.
http://www.ciscopress.com

- PACKET
Revista para el usuario técnico de Cisco Systems para la maximización de las inversiones en redes de Internet. Cada trimestre, Packet brinda cobertura de las últimas tendencias del sector, las novedades tecnológicas y los productos y las soluciones Cisco, así como sugerencias para implementación y solución de problemas, ejemplos de configuración, estudios de casos de clientes, información sobre certificación y formación, y enlaces a un gran número de recursos exhaustivos de Internet.
http://www.cisco.com/packet

- IQ Magazine
Publicación trimestral de Cisco Systems diseñada para ayudar a las compañías en crecimiento a aprender a utilizar la tecnología para aumentar sus ingresos, facilitar sus negocios y ampliar sus servicios. La publicación identifica los desafíos a los que se enfrentan estas empresas y las tecnologías que las ayudan a superarlos, por medio de estudios de casos reales y estrategias comerciales, para que los lectores puedan tomar decisiones acertadas respecto de la inversión en tecnología.
http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal
Periódico trimestral que edita Cisco Systems, destinado a profesionales en el campo de la ingeniería relacionados con el diseño, el desarrollo y la utilización de Internet e Intranets públicas y privadas.
http://www.cisco.com/ipj

- Cisco Systems Latinoamérica–Redacción Virtual
En RedacciónVirtual.com encontrará información actualizada y relevante sobre las actividades de Cisco en el mundo y la región latinoamericana, la industria de la conectividad y las implicaciones de la tecnología en la sociedad.
http://www.ciscoredaccionvirtual.com/redaccion/default.asp









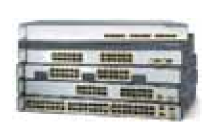
FOTO: (c) JUPITERIMAGES, and its Licensors. All Rights Reserved

Guía de referencia rápida de productos Cisco



SWITCHES NIVEL 3 QoS - Seguridad

Cisco Catalyst® 3750



La serie de switches Catalyst® 3750 es una línea de productos innovadores que mejoran la eficiencia en las redes LAN combinando el desempeño, con la arquitectura de mas alta disponibilidad. Representan la nueva generación de switches con servicios avanzados de QoS para aplicaciones como Telefonía IP y video por Streaming con multicast. La tecnología Cisco StackWise™ utiliza una interconexión de apilamiento de 32-Gbps permitiendo definir un sistema escalable y ajustable a las necesidades crecientes de ancho de banda. La familia de equipos 3750 viene con dos versiones de Sistema operativo IOS, Standard Multilayer Image SMI con rutas estáticas y RIP o una versión más completa de IOS Enhanced Multilayer Image EMI con OSPF, EIGRP, o BGP. La arquitectura utilizada soporta Ipv6.

WS-C3750G-12S-E / S



12 10/100/1000 + 1 10GbE XENPAK, 35,7 Mpps
StackWise™. Distancias desde 15 metros por Cobre, 300 metros para fibra multimodo y hasta 40km con fibra monomodo con Xenpak. software SMI y EMI.

WS-C3750G-12S-S / S



12 SFP Slots 17,8 Mpps
fibra Monomodo, multimodo o UTP en SFP Slots . Apilamiento StackWise™ 32Gbps. Servicios inteligentes de red y seguridad como QoS, 802.1X, SSH. Enrutamiento IP estático y dinámico con RIP, OSPF, EIGRP, BGP con el IOS respectivo.

WS-C3750G-48TS-E / S



48 10/100/1000T + 4 SFP Slots. 38,7 Mpps 1.5 RU. StackWise™32 Gbps. Servicios inteligentes de red QoS, 802. 1X, enrutamiento IP estático y dinámico RIP, OSPF, EIGRP, BGP.

WS-C3750G-24TS-E1U / S1U



24 10/100/1000T + 4 SFP Slots. 38,7 Mpps. 1 RU. Uplinks fibra o cobre StackWise™
32 Gbps. Servicios inteligentes de red QoS, 802. 1X, enrutamiento IP estático y dinámico RIP, OSPF, EIGRP, BGP.

WS-C3750G-24T-E / S



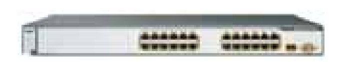
24 0/100/1000. 32Gbps, 35.7Mpps Apilamiento StackWise™ a 32Gbps. QoS, 802.1X, SSH. Switch de nivel 3 para enrutamiento IP estático y dinámico con RIP, OSPF, EIGRP, BGP con el IOS respectivo.

WS-C3750-48TS-E / S



48 10/100 + 4 SFP Slots para 32Gbps, 13.1 Mpps. Uplink UTP, fibra multimido monomodo. Nivel 3 con rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP, PIM. Apilamiento a 32 Gbps con StackWise.

WS-C3750-24TS-E / S



24 10/100 + 2 Slots SFP , 32Gbps, 6.5Mpps Uplink fibra multimodo, Monomodo (500mts - 70Kmts) Nivel 3 con rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP, PIM. Apilamiento a 32 Gbps.

Cisco Catalyst® 3560

Los switches Cisco Catalyst 3560 Series son de configuración fija, Enterprise-Class que incluyen puertos FastEthernet o GigabitEthernet 10/100/1000 y/o Power over Ethernet permitiendo la implementación de nuevas aplicaciones como Telefonía IP, Wireless, Video Kioscos etc. Las compañías pueden implementar servicios inteligentes de red como rate-limiting, ACL, Multicasting y enrutamiento de alto desempeño. Cisco Catalyst 3560 Series vienen con Cisco Network Assistant el cual simplifica las tareas de administración incluyendo routers y AP inalámbricos para redes convergentes. IOS Standard Multilayer Image SMI que permite tener rutas estáticas y RIP o IOS Enhanced Multilayer Image EMI para protocolos más complejos como OSPF, EIGRP, PIM o BGP.

WS-C3560G-48TS- E / S



48 10/100/1000T + 4 SFP Slots. 32Gbps, 38,7 Mpps. Uplink Fibra o Cobre.Servicios Inteligentes de Red, QoS, Multicasting, Rate-limiting, SSH, 802.1X

WS-C3560G-24TS- E / S



24 10/100/1000T + 4 SFP Slots. 32Gbps, 38,7 Mpps. Uplink Fibra o Cobre Servicios Inteligentes de Red, QoS, Multicasting, Rate-limit, SSH, 802.1X

Cisco Catalyst® 3550

Los Switches Inteligentes Ethernet Cisco Catalyst® 3550 están enfocados a soluciones empresariales, apilables, con necesidades de enrutamiento entre VLANs a nivel 3. Ofrece alta disponibilidad, seguridad y QoS para mejorar la operación de la red. Hay varias opciones de configuración con puertos FastEthernet y Gigabit Ethernet. Las compañías pueden implementar servicios inteligentes a través de la red para garantizar que las aplicaciones de voz y video sobre IP funcionen óptimamente, límites de tráfico para controlar ancho de banda , listas de control de acceso ACL, manejo de multicast, alto desempeño enrutando IP mientras se mantiene la simplicidad de las redes LAN tradicionales. La familia de equipos 3750 viene con dos versiones de Sistema operativo IOS, Standard Multilayer Image SMI que permite tener rutas estáticas y RIP o una versión más completa de IOS Enhanced Multilayer Image EMI para protocolos más complejos como OSPF, EIGRP, PIM o BGP.

WS-C3550-12G



10 Slots 1000BASE-X GBIC + 2 10/100/1000BASE-T. 24 Gbps, 17Mpps Switch Gigabit Ethernet de Nivel 3 para UTP, fibra multimodo o monomodo. Agregación de puertos 802.1ad. Rutas estáticas, RIP, OSPF, EIGRP, BGP. Servicios inteligentes de red como QoS y seguridad.

WS-C3550-12T



10 10/100/1000BASE-T + 2 Slots 1000BASE-X.24 Gbps, Ideal como equipo concentrador de switches de pisos por UTP o granja de servidores. Agregación de puertos 802.1ad para aumentar ancho de banda. Rutas estáticas, RIP, OSPF, EIGRP, PIM, BGP.

WS-C3550-48-SMI / EMI



48 10/100 + 2 Slots 1000BASE-X GBIC. 13.6 Gbps, 10.1Mpps. Uplink en UTP, fibra monomodo o multimodo. Enrutamiento estático y dinámico con RIP, OSPF, EIGRP, BGP. Límites de tráfico para controlar anchos de banda de acceso al Backbone, además de servicios inteligentes de red.

Imágenes pertenecientes al banco de imágenes de Cisco Systems, Inc. Todos los derechos reservados.

WS-C3550-24-SMI / EMI



24 10/100 + 2 Slots 1000BASE-X GBIC. 8.8 Gbps, 6.6 Mpps. Uplink UTP o fibra monomodo, multimodo alcanzando distancias de hasta 70 Km. Switch nivel 3 con rutas estáticas y RIP con IOS SMI o dinámicas con OSPF, EIGRP, BGP con EMI.

WS-C3550-24-FX-SMI



24 100BaseFX MM + 2 Slots 1000BASE-X GBIC 8.8 Gbps por UTP o Fibra multimodo o monomodo. Ideal para compañías que mantienen un backbone en fibra a 100Mbps. Enrutamiento estático y dinámico.

SWITCHES NIVEL 3 Power Over Ethernet PoE 802.3af



Son una serie de switches de configuración fija disponible en las familias Catalyst 3750 y Catalyst 3560. Cumplen con el Standard IEEE 802.3af PoE y el pre-standard Cisco Power over Ethernet en puertos FastEthernet o GigabitEthernet, Proven 48 VDC por el cable RJ-45 a dispositivos como teléfonos IP, Access Point, Cámaras de Video IP etc. Ofrecen alta disponibilidad, seguridad y calidad de servicios QoS para mejorar la operación de la red. La tecnología CiscoStackWise™ utiliza una interconexión de apilamiento de 32-Gbps permitiendo definir un sistema escalable y ajustable a las necesidades crecientes de ancho de banda.

Cisco Catalyst® 3750 PoE

WS-C3750G-48PS-E / S



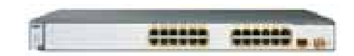
48 10/100/1000T 802.3af + 4 SFP Slots. 32Gbps. 38,7 Mpps StackWise™ QoS, 802.1X, SSH. Enrutamiento IP estático SMI y dinámico EMI con RIP, OSPF, EIGRP, BGP.

WS-C3750G-24PS-E / S



48 10/100 802.3af + 4 SFP Slots.32Gbps. 13,1 Mpps StackWise™ QoS, 802.1X, SSH. Enrutamiento IP estático SMI y dinámico EMI con RIP, OSPF, EIGRP, BGP

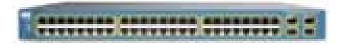
WS-C3750-24PS-E / S



24 10/100 802.3af + 2 SFP Slots. 32Gbps. 6,5 Mpps StackWise™ QoS, 802.1X, SSH. Enrutamiento IP estático SMI y dinámico EMI con RIP, OSPF, EIGRP, BGP.

Cisco Catalyst® 3560 PoE

WS-C3560G-48PS-E / S



48 10/100/1000T 802.3af + 4 SFP Slots. 32Gbps, 38,7Mpps Uplink fibra multimodo, monomodo(500mts -70Kmts). Enrutamiento con rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP, PIM.

WS-C3560G-24PS-E / S



24 10/100/1000T 802.3af + 4 SFP Slots.32Gbps, 38,7Mpps. Uplink fibra multimodo, monomodo (500mts -70Kmts) Enrutamiento con rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP, PIM.

WS-C3560-48PS-E / S



48 10/100 802.3af + 4 SFP Slots. 17.6Gbps, 13.1Mpps Uplink fibra multimodo, monomodo (500mts -70Kmts) Enrutamiento con rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP

WS-C3560-24PS-E / S



24 10/100 802.3af + 2 SFP Slots.8.8Gbps, 6.6Mpps Uplink fibra multimodo, monomodo(500mts -70Kmts) Rutas estáticas y dinámicas con RIP, OSPF, EIGRP, BGP, PIM.

SWITCHES NIVEL 2 QoS - Seguridad

Cisco Catalyst® 2970



Switches Gigabit Ethernet, Wire-Speed con servicios inteligentes de red, seguridad mejorada para proteger los dispositivos interconectados, QoS avanzada para transporte de voz , video y datos por IP. Fácil implementación y configuración con Cluster Management Suite y el Nuevo Express Setup. Cisco IOS® Software. Implementa Cisco ASICs para mejorar el desempeño. Gigabit al escritorio.

WS-C2970G-24TS-E

24 10/100/1000 + 4 Slots GBIC SFP, 28Gbps, 38.7Mpps. Uplink para fibra multimodo y monomodo. Servicios inteligentes de red en nivel 2 802.1s/w, limites de tráfico, QoS y Seguridad. Autenticación con 802.1X, VLAN dinámicas ACL listas de control de acceso Wire-Speed, port security, SSH, SNMPv3. Manejo inteligente de Multicast IGMP snooping. Implementación de Gigabit al escritorio.

WS-C2970G-24T-E



24 10/100/1000. 24Gbps, 35.7Mpps. Wire-speed switching. Servicios inteligentes de red en nivel 2 802.1s/w, limites de tráfico, QoS y Seguridad. Autenticación con 802.1X, VLAN dinámicas ACL listas de control de acceso Wire-Speed, port security, SSH, SNMPv3. Manejo inteligente de Multicast, IGMP snooping. Implementación de Gigabit al escritorio.

Cisco Catalyst® 2950



Switches de configuración fija, apilables y standalone con FastEthernet y Gigabit Ethernet. Servicios avanzados e inteligentes de red como QoS, Seguridad y manejo de Multicast. Interconexión con varios tipos de medio Cobre o Fibra. Fácil configuración de los servicios inteligentes de red. Administración de hasta 16 Switches Catalyst como 37XX/35XX/29XX con la herramienta gráfica Cluster Management Suite. Dos versiones IOS Standard Image SI con QoS: CoS, 4 queues y WRR Multiples instancias de STP, 64 VLAN, 802.1X, port security e IGMP Snooping, y IOS Enhanced Image EI con QoS L2-4, 802.1s/w, rate-limit 1Mbps, RSPAN. Apilamiento con GigaStack.

WS-C2950G-48-EI



48 10/100 + 2 Slots GBICs, 13.6Gbps, 10.1Mpps.Uplinks y apilamiento con GigaStack. Alta disponibilidad con STP mejorado, 802.1s/w, IGMP snooping. Seguridad con 802.1X, ACPs, Port Security, notificación de MAC, RADIUS/TACACS+, SSH, SNMPv3. Servicios de QoS L2-L4 con CoS/ToS, colas de prioridad, límites de tráfico, Auto-QoS para VoIP. Administración gráfica con Cluster Management Suite.

WS-C2950G-24-EI



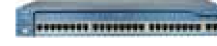
24 10/100 + 2 Slots GBICs, 8.8 Gbps, 6.6Mpps Uplinks en fibra o UTP y apilamiento GigaStack. Alta disponibilidad con STP mejorado, 802.1s/w, IGMP snooping. Seguridad con 802.1X, ACPs, Port Security, notificación de MAC, RADIUS/TACACS+, SSH, SNMPv3. Servicios de QoS L2-L4 con CoS/ToS, colas de prioridad, limites de trafico, Auto-QoS para VoIP.

WS-C2950G-12-EI



12 10/100 + 2 Slots GBICs, 6.4Gbps, 4.8Mpps Uplinks fibra o UTP y apilamiento con GigaStack Alta disponibilidad con STP mejorado 802.1s/w, IGMP snooping. Seguridad con 802.1X, ACLs, Port Security, notificación de MAC, RADIUS/TACACS+, SSH, SNMPv3. Servicios de QoS L2-L4 con CoS/ToS, colas de prioridad, límites de tráfico, Auto-QoS para VoIP.

WS-C2950T-24



24 10/100 + 2 10/100/1000, 8.8Gbps, 6.6 Mpps Alta disponibilidad con STP mejorado, 802.1s/w, IGMP snooping. Seguridad mejorada con 802.1X, ACLs, Port Security, notificación de MAC, RADIUS/TACACS+, SSH, SNMPv3. Servicios de QoS L2-L4 con CoS/ToS, colas de prioridad, limites de tráfico, Auto-QoS para VoIP. Administración gráfica con Cluster Management Suite.

WS-C2950C-24



24 10/100 + 2 100 Base FX, 5.2Gbps, 3.9Mpps Alta disponibilidad con STP mejorado, 802.1s/w, IGMP snooping. Seguridad mejorada con 802.1X, ACLs, Port Security,notificación de MAC, RADIUS/TACACS+, SSH, SNMPv3. Servicios de QoS L2-L4 con CoS/ToS colas de prioridad, limites de tráfico, Auto-QoS para VoIP. Administración gráfica con Cluster Management Suite.

WS-C2950SX-24



24 10/100 + 2 1000BaseSX, 8.8Gbps, 6.6Mpps Fibra multimodo de uplink, configuración fija, redes pequeñas y medianas. Administrable con SNMP y la herramienta gráfica Cluster Management Suite. Clasificación de paquetes basados en 802.1p CoS y colas de prioridad. VLANs dinámicas y 802.1x.

WS-C2950-24



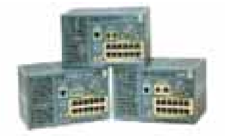
24 10/100, 4.8Gbps, 3.6Mpps Standalone, configuración fija, Redes pequeñas y medianas. Administrable con SNMP y la herramienta gráfica Cluster Management Suite. Clasificación de paquetes basados en 802.1p CoS y colas de prioridad. VLANs dinámicas y 802.1x.

WS-C2950-12



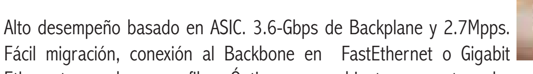
12 10/100, 2.4 Gbps, 1.8Mpps Standalone, configuración fija, conectividad para redes pequeñas y medianas. Administrable con SNMP y la herramienta gráfica Cluster Management Suite. Clasificación de paquetes basados en 802.1p CoS y colas de prioridad. VLANs dinámicas y 802.1x.

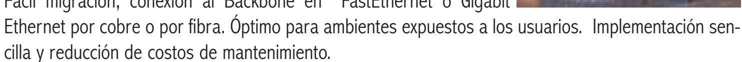
WS-C2955C-12, S-12, T-12



2 10/100 + 2 Uplink 100 FX Multimodo o monomodo o 2 10/100/1000 por UTP. 13.6Gbps, 4 Mpps. Hardware optimizado para operación en Industrias. No tiene ventiladores. Enfriamiento por convección, diseño térmico avanzado para peso reducido, Operación segura, Sensores detemperatura, SNMP y herramienta gráfica Cluster Management Suite. Clasificación 802.1p CoS y colas de prioridad.

Cisco Catalyst® 2940





Alto desempeño basado en ASIC. 3.6-Gbps de Backplane y 2.7Mpps. Fácil migración, conexión al Backbone en FastEthernet o Gigabit Ethernet por cobre o por fibra. Óptimo para ambientes expuestos a los usuarios. Implementación sencilla y reducción de costos de mantenimiento.

WS-C2940-8TT-S



8 10/100 + 1 10/100/1000T. Conmutación a través de ASICs. Aseguramiento físico, múltiples maneras de instalación. Servicios inteligentes de QoS, Seguridad con 802.1x, RADIUS. Filtrado por direcciones MAC, Administración gráfica vía Web a través del Cisco Express Setup.

WS-C2940-8TF-S



8 10/100 + 1 100BASE-FX o 1 SFP Slot. Solo un puerto activo de uplink o 100BaseFX o SFP. Conmutación a través de ASICs. Aseguramiento físico. Servicios inteligentes de QoS, 802.1x, RADIUS. Filtrado por direcciones MAC, Administración vía Web con Cisco Express Setup

Cisco Catalyst® 2950 Long Reach Ethernet LRE



La solución LRE permite conectividad Ethernet sobre cable telefónico categoría 1, 2, 3. Coexiste con los sistemas telefónicos tradicionales POTS, ISDN o PBX sobre el mismo cable. Variedad de perfiles de conexión de 2 - 15Mbps para distancias de hasta 1500mts. Utiliza VDSL y modulación digital con Ethernet.Transmisión Punto-Punto simétrico, full-duplex 15Mbps .Agregación de enlaces.

WS-C2950ST-8-LRE, 24-LRE



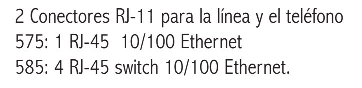
8 o 24 Puertos LRE + 2 SFP Slots o 2 10/100/100. Conector RJ-21 Amphenol. Funciona el puerto SFP o el 10/100/1000 simultaneo. SSH, 802.1x, QoS L2-4, VLANs, 802.1Q. Perfiles de 2-15 Mbps por puerto LRE.

PS-1M-LRE-48



48 Puertos en 1 Unidad de Rack, RJ-21. Permite coexistir LRE con PBX , POTS.

CISCO575-LRE o 585-LRE







2 Conectores RJ-11 para la línea y el teléfono
575: 1 RJ-45 10/100 Ethernet
585: 4 RJ-45 switch 10/100 Ethernet.

ROUTERS DE SERVICIOS INTEGRADOS ISR

Cisco Routers 3800



Los routers 3800 son diseñados para pequeñas y grandes compañías.

La familia 3800 consiste en 2 nuevas plataformas modulares, optimizadas para manejo de servicios de datos, voz y video concurrentes de manera segura. Cisco 3825 y 3845 están disponibles en tres opciones de alimentación AC, AC integrados con alimentación 802.3af para Teléfonos IP y DC. La serie 3800 soporta altos y medianos requerimientos de ancho de banda WAN con alta densidad de servicios, interconexiones TDM, potencia para 802.3af sobre Ethernet, manteniendo compatibilidad con los módulos actuales .Garantiza protección a la inversión permitiendo expansiones y cambios tecnológicos como nuevos servicios y aplicaciones.

Cisco3845



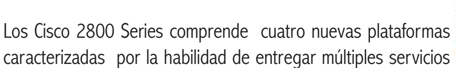
2 10/100/1000T o 1 SFP Slot, 4 HWIC Slots
4 NME/EVM (2 Max EVM / 2 NME Doble Capacidad)
4 PVDM2 Slots, 2 AIM Slots, 2 USB Port , 1 Aux Port, 1 Consola
256M RAM / 64M Flash, MAX (1GB RAM / 256M Flash)

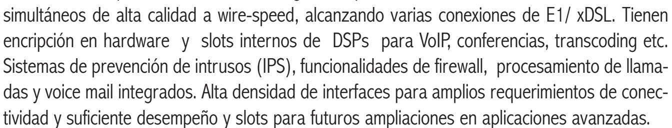
Cisco3825



2 10/100/1000T o 1 SFP Slot, 4 HWIC Slots 3
NME/EVM (1 Max EVM / 1 NME Doble Capacidad)
4 PVDM2 Slots, 2 AIM Slots, 2 USB Port, 1 Aux Port, 1 Consola
256M RAM / 64M Flash, MAX (1GB RAM / 256M Flash)

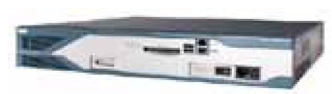
Cisco Routers 2800





Los Cisco 2800 Series comprende cuatro nuevas plataformas caracterizadas por la habilidad de entregar múltiples servicios simultáneos de alta calidad a wire-speed, alcanzando varias conexiones de E1/ xDSL. Tienen encripción en hardware y slots internos de DSPs para VoIP, conferencias, transcoding etc. Sistemas de prevención de intrusos (IPS), funcionalidades de firewall, procesamiento de llamadas y voice mail integrados. Alta densidad de interfaces para amplios requerimientos de conectividad y suficiente desempeño y slots para futuros ampliaciones en aplicaciones avanzadas.

Cisco2851



2 10/100/1000T, 4 HWIC Slots
1 EVM Slot, 2 NME (1 NME Doble Capacidad)
3 PVDM2 Slots, 2 AIM Slots, 2 USB Port, 1 Aux Port, 1 Consola
256M RAM / 64M Flash, MAX (1GB RAM / 256M Flash)

Cisco2821

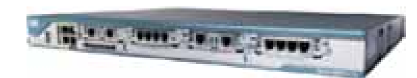
2 10/100/1000T, 4 HWIC Slots
1 EVM Slots, 1 NME
3 PVDM2 Slots, 2 AIM Slots, 2 USB Port, 1 Aux Port, 1 Consola
256M RAM / 64M Flash, MAX (1GB RAM / 256M Flash)

Cisco2811



2 10/100, 4 HWIC Slots, 1 NME
2 PVDM2 Slots, 2 AIM Slots, 2 USB Port, 1 Aux Port, 1 Consola
256M RAM / 64M Flash, MAX (670MB RAM / 256M Flash)

Cisco2801

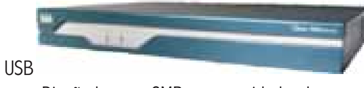


2 10/100, 2 HWIC Slots
1 VWIC/WIC/VIC Slot, 1 VWIC/VIC Slot
2 PVDM2 Slots, 2 AIM, 1 USB Port, 1 Aux Port, 1 Consola
128M RAM / 64M Flash, MAX (384MB RAM / 128M Flash)

Cisco Routers 1800

Cisco 1800 ISR son routers de servicios integrados y la nueva generación de los Cisco 1700. Esta diseñado para lograr la seguridad de la información utilizando encripción basada en hardware, soportada por Cisco IOS Software Security. Creado para compañías pequeñas y medianas o sucursales de grandes empresas con necesidades de conectividad y seguridad de manera concurrente. Con los 1800 las empresas pueden tener firewall, prevención de intrusos IPS, VPN IPSEC configurables a través de la herramienta grafica basada en WEB Security Device Manager.

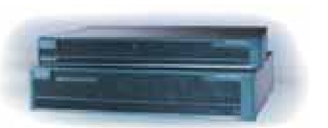
Cisco Routers 1841



2 10/100, 2 HWIC Slots 1 AIM Slot, 1 USB Port, 1 Aux Port, 1 Consola Desk Form Factor. Diseñado para SMB en seguridad y datos.

ROUTERS ACCESO CISCO

Cisco Routers 3700



Los routers de acceso Cisco cumplen con los requerimientos de servicios de las sucursales remotas "The Full Service Branch". Una plataforma flexible para Telefonía IP y Gateway de voz. Integración de enrutamiento con Switching de baja densidad. Protección de inversión con interoperabilidad de módulos de los routers 3600/2600/1700. Los routers 3700 tienen la funcionalidad de CallManager Express para Telefonía IP, Gatekeeper, Firewall, VPNs, Detección de Intrusos, RAS con E1 PRI y BRI además de los servicios tradicionales de enrutamiento con protocolos como RIP, OSPF, EIGRP, BGP, PIM, GRE etc.

CISCO3745



2 10/100 + 3 Slots WIC + 4 Slots Network Modules (2 Doble capacidad) 2 Slots AIM + Puerto AUX Consola, 32 MBytes Flash (Upgrade 128), Slot PCMCIA para Flash. 128 RAM (Upgrade 256 MBytes). 225 Kpps. Routers de más alto desempeño para sucursales remotas. Interfaces seriales V.35, RS-232, E1 PRI o R2, BRI , ATM , Gigabit Ethernet, switching de Baja densidad 16 o 36 Puertos Ethernet. Firewall, VPN IPSEC, Sistemas de Detección de Intrusos, Cache.

CISCO3725

2 10/100 + 3 Slots WIC + 2 Slots Network Modules (1 Doble Capacidad) 2 Slots AIM + Puerto AUX 1 Consola, 32 MBytes Flash (Upgrade 128), Slot PCMCIA para Flash. 128 RAM (Upgrade 256 MBytes). 100Kpps Routers de mas alto desempeño para sucursales remotas. Interfaces seriales V.35, RS-232, E1 PRI o R2, BRI , ATM , Gigabit Ethernet, Switch de Baja densidad 16 o 36 Puertos Ethernet. Firewall, VPN IPSEC, Sistemas de Detección de Intrusos, Cache.

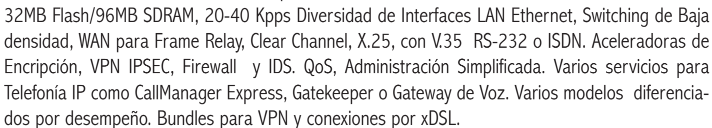
Cisco Routers 2691/2600XM

CISCO2691

2 10/100 + 1 Network Module + 3 Slot WIC
2 Slots AIM Puerto AUX + Consola + PCMCIA para Flash. Default-32MB Flash/128MB SDRAM.
70 Kpps. Diversidad de Interfaces LAN, WAN , ISDN. Aceleradoras de Encripción, VPN, Firewall y Detección De Intrusos. QoS, Administración Simplificada.

CISCO2600XM

1 o 2 10/100 + 1 Network Module + 2 Slots WIC, 1 Slots AIM Puerto AUX + Consola + PCMCIA para Flash. Default-32MB Flash/96MB SDRAM, 20-40 Kpps Diversidad de Interfaces LAN Ethernet, Switching de Baja densidad, WAN para Frame Relay, Clear Channel, X.25, con V.35 RS-232 o ISDN. Aceleradoras de Encripción, VPN IPSEC, Firewall y IDS. QoS, Administración Simplificada. Varios servicios para Telefonía IP como CallManager Express, Gatekeeper o Gateway de Voz. Varios modelos diferenciados por desempeño. Bundles para VPN y conexiones por xDSL.



Cisco Routers 800/SOHO

CISCO800

Los routers Cisco 800 son útiles para Teletrabajadores o pequeñas oficinas de hasta 20 Usuarios que requieren conectividad y seguridad. Equipos fijos con varias opciones Ethernet, ISDN, Dual Ethernet, WAN, HUBs, xDSL con funcionalidades de VoIP, Firewall, VPN, NAT, Servidor DHCP. Servicios de IP conprotocolos de enrutamiento como EIGRP, Multicast, Listas de Control de Acceso, Algoritmos de QoS (LLQ), CAR.

CISCO SOHO

Acceso a Internet Seguro para oficinas pequeñas o uso residencial. Acceso a Internet seguro con Firewall Inspection. Fácil de configurar e implementar con Cisco Router Web Setup Tool vía Web. Varias opciones de conectividad con Ethernet, ADSL o G.SHDSL ADSL over ISDN y Hubs de Ethernet. IPSec Pass-through. Servicios de IP como MAC address y hostname pass-through para Cable Modems, lista de Control de Acceso por IP, TCP o UDP, NAT, PAT, PPPoE, DHCP Cliente/Server, Telnet, SNMPv3. Autenticación PAP/CHAP. IGRP, RIP, EIGRP. Versión de IOS IP/FW Stateful.

MODULOS ROUTERS

Los routers tiene la posibilidad de utilizar diferentes medios de conexión como Módulos de 4, 8,16,32 puertos asincrónicos, 1 o 2 E1 PRI para RAS o Gateway de Voz, puertos Análogos FXS, FXO, E&M. 1, 2, 8, 16 Modems análogos, Interfaces HSSI, ATM, Ethernet, FastEthernet, Gigabit Ethernet, aceleradores de Encripción, servicios avanzados de red como IDS, Cache, Correo de Voz etc. Los GBICs le dan la opción a los Switches de escoger el tipo de Medio físico y la distancia de conexión con Fibra Monomodo y Multimodo (550mts, 10 Km o 70Km) o cobre. Switches de baja densidad dentro de los routers.

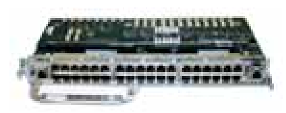
NM-1GE

1 Gigabit Slot para cobre o fibra hasta 70 Km con GBICs. Enrutamiento entre VLAN, 802.1q e ISL. QoS jerárquico y Jumbo Frames.



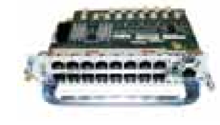
NMD-36-ESW

36 10/100 autosensing Switch; Full-Half duplex. Utiliza 2 Network Modules Slots. Power over Ethernet para Teléfonos IP con modulo adicional. Uno o dos Gigabit Ethernet para Uplinks.



NM-16ESW

16 10/100 autosensing Switch. Full-Half duplex Power over Ethernet para IP Phones o AP.



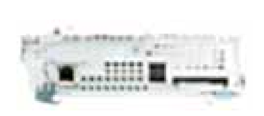
NM-CIDS-K9

45 Mbps. Integración completa de IDS con una variedad de Routers Cisco. Monitorea todas las interfaces del router. Analiza tráfico desencriptado GRE/IPSEC después del router. Administración Web.



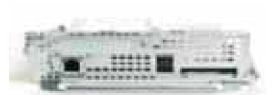
NM-CE-BP-40G-K9

Caching Transparente, Filtrado de Contenido. RADIUS, LDAP, TACACS+. Soporte de video por streaming MPEG, Windows Media, Realnetworks, QuickTime. External Storage SCSI Adapter.



NM-NAM

Network Analisys Module permite monitorear trafico por aplicacion, host, puertos etc. Monitoreo VoIP. Reportes via WEB. CPU independiente



NM-CUE

Cisco Unity Express para Routers. Operadora automática. Sistema de Voice Mail 12-100 Mailboxes, 4-8 Sesiones 100 Horas de almacenamiento.



EVM-HD-8FXS/DID

8 FXS, 2 Expansion Module Slots. Cisco 2821, 2851, 3825, 3845. Puertos análogosde Voz/FAX, Conector RJ-21 Amphenol. Expansiones de 6FXO, 8FXS, 3FXS/4FXO, 4BRI.



NM-HDA-4FXS

4 Puertos FXS , Alta densidad de puertos análogos de Voz/FAX, Conector RJ-21 Amphenol. Hasta 8 FXO o 12 FXS, VoIP H.323, VoIP SIP.



NM-HD-1V, 2V, 2VE

3 Network Modules con mayor densidad de puertos de voz combinando análogos y digitales E1. Routers 26/36/3700, VoIP, VoFR, VoATM.



NM-HDV2-1T1/E1 o 2 T1/E1

Modulo de Gateway de Voz.1 o 2 E1 con codecs. Para algoritmos mediana y alta disponibilidad, Granja de DSP para funcionalidades de Transcoding y conferencia



NM-8AM-V2 o NM-16AM-V2

8 o 16 Modem Análogos RJ-11.Protocolos V.90, V.92, V.44 soportados Modem Firmware Actualizable sin reboot Fax-out Class 2





NM-30DM, 24, 18, 12, 6.

6, 12, 18, 24 o 30 Modems Digitales para terminar llamadas originadas en líneas análogas por Dial-Up.



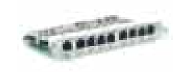
VIC2-2FXS o 2E&M

2 Puertos FXS para teléfonos análogos,
FAX o para interconexión con PBX o Key Systems.



VIC2-2FXO o VIC2-4FXO

2 o 4 Puertos FXO para interconexión con PBX, Key Systems, o PSTN.



HWIC-4ESW

4 10/100 Switch. Opcion de Power Over Ethernet y 802.3af. 2 Por Chasis.



HWIC-D-9ESW

8 10/100 Puertos Acceso, 1 10/100 Stack o uplink
Opción de Power Over Ethernet y 802.3af.
2 Por Chasis. Auto-MDIX



HWIC-1GE-SFP

1 SFP Slot. SFP para fibra o cobre.1 o 2 por chasis segun modelo.
Cisco 2811,2821, 2851, 3800.



WIC-1ENET

1 Ethernet para Slots WIC en routers1700.



WIC-4ESW

4 10/100 Ethernet Switch. Cisco 1700 802.1Q para VLANs
y 802.1p. Spanning Tree.1 Modulo por Router. Auto-MDIX



WIC-1AM o 2AM

1 o 2 Modem Análogos, V.90 Dial-in V.34+ (33.6k);
Dial-out V.90 (56k) Dial-out FAX 9.6k, 14.4k.
Soporte PPP Multilink para agrupar múltiples líneas telefónicas.



WIC-1B-S/T-V3

Interface BRI para conexión para enlace dedicado o por dial para backup.



WIC-1T o 2T

Puertos Seriales de alta velocidad RS-232,
V.35 con conectores DB-60 o Smart Serial.



WIC-1ADSL o G.SHDSL

Múltiples tarjetas por Chasis
Soporte QoS para ATM e IP. 1700/2600/3600/3700.



AIM-CUE

Cisco Unity Express, 12 Mailbox. Interactua con CallManager
y CallManager Express. 4 Horas de Almacenamiento.
Cisco 2801, 281X, 282X, 285X and 2691, 2600XM, 3700
4 Sesiones simultaneas.



SEGURIDAD Self Defending Networks

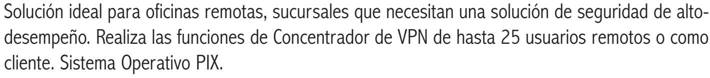
PIX FIREWALL

La Serie de PIX Firewall ofrece la seguridad necesaria en ambientes empresariales para oficinas remotas o sucursales. Dispositivos confiables, con un amplio rango de características de seguridad como Firewall, VPN, IDS dentro de un solo dispositivo. Opciones de alta disponibilidad para garantizar alta disponibilidad con una solución de alto desempeño. Herramienta Gráfica de Administración para todos PIX DEVICE MANAGER.

PIX-501

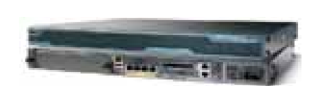
1 Ethernet para Internet + 4 10/100 Switch para PCs internos. Firewall para redes de pequeñas oficinas, teletrabajadores y conexiones a Internet por Banda Ancha(Cable/ DSL). Realiza las funciones de Clientes de VPN IPSEC. Configuración de Fábrica Plug & Play Configuración vía Web con Ayudas.

PIX-506



1 Ethernet a Internet + 1 Ethernet a Intranet.
Solución ideal para oficinas remotas, sucursales que necesitan una solución de seguridad de alto-desempeño. Realiza las funciones de Concentrador de VPN de hasta 25 usuarios remotos o como cliente. Sistema Operativo PIX.

PIX-515E



Solución para la pequeña y mediana empresa con requerimientos de un dispositivo de alto desempeño con Zonas desmilitarizadas DMZ y alta disponibilidad con Failover. Soporte de hasta 6 Interfases 10/100. Concentrador y cliente de VPN con tarjeta aceleradora de Encripción. Sistema Operativo PIX.

Cisco Intrusion Prevention System

IPS-4240-K9 / IPS-4255-K9

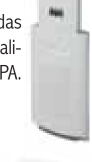
Inline Network Intrusion Prevention ofrece la Confianza para detener trafico malicioso. Múltiples mecanismos de reacción TCP Reset, Inline Drop,Blocking Host, SNMP Traps, Packet logging, basados en Valoración de Riesgo como Severidad, Fidelidad de las firmas, Relevancia del Ataque y de la infraestructura comprometida para disminuir Falsas Alarmas e incrementar la exactitud

Cisco Security Agent

Cisco Security Agent va más allá de las soluciones de seguridad para desktop convencionales como Firewall personales e IDS para Hosts, identifica y previene comportamiento anormal y malicioso, logrando remover las amenazas sobre la red o las aplicaciones ya sean riesgos conocidos o desconocidos. Cisco Security Agent analiza el comportamiento aun mas que comparar firmas reduciendo los costos operativos de actualización de las mismas.

WIRELESS LAN 802.11a/b/g

AIR-AP1120B-A-K9 o AIR-AP1121G-AK9



Acces Point para 2.4 Ghz en 802.11b actualizable a 8002.11g. Antenas integradas de 2.2 dbi y 100 mW de potencia de transmición. Power Over Ethernet para la alimentación. Más alto desempeño en la industria. 802.1X con LEAP, PEAP, TKIP y WPA. Soporte de VLAN inalámbricas y mejoras para VoWLAN.

AIR-AP1131AG-A-K9



Dual Radio para 802.11g y 802.11a, hasta 56 Mbps. Outdoor AP con antenas integradas con cubrimiento. Omnidireccional. Cisco PoE y 802.3af. Cisco IOS Software.

AIR-AP1200



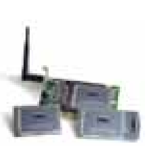
Acces Point Dual-Band 2.4 Ghz y 5Ghz 8002.11b, 802.11a, 802.11g. Varias Opciones de antenas que se conectan a los conectores externos para 2.4 Ghz y 100 mW de potencia. Antenas integradas de 6dbi de ganancia para 5Ghz. Power over Ethernet para la alimentación. Más altodesempeño en la industria. 802.1X con LEAP, PEAP, TKIP, y WPA. VLAN inalámbricas, QoS para VoWLAN.

AIR-BR1310G-A-K9 o AIR-BR1310G-A-K9-R



Bridge Inalámbrico para 54 Mbps 802.11g. Con antenas integradas de 13dbi o para antenas remotas. Cisco IOS Software. Punto-Punto o Punto-Multipunto. AP Outdoor. Hasta 4.5 miles @ 54 Mbps o ¡4 miles @ 11 Mbps

TARJETAS CLIENTES



PCMCIA, PCI en 802.11b o CardBus para 802.11a. 802.11a/b/g
PCI o Card Bus. WorkGoupBridge para Impresoras o equipos con puertos ethernet. Sistemas operativos Windows 95, 98, ME, NT 2000,XP, LINUX, MAC OS 9.X. Múltiples perfiles para facilidad de cambiar de redes inalámbricas Con Aironet Client Utilities o para realizar el Site Survey.

ANTENAS



Amplia gama de antenas entre Omnidireccionales, Direccionales. Diferentes ganancias permiten ajustarse a los requerimientos de cada sitio específico para lograr la zona de cobertura adecuada en frecuencias de 2,4GHz o 5,7GHz

ACCESORIOS



Power Injector para alimentar AP con Cisco PoE, cables de baja perdida con conectores RP-TNC de 20, 50, 100 pies, protecciones contra descargas, montaje en rack etc.



www.cisco.com/go/isr
www.cisco.com/go/irschannel
www.cisco.com/go/safe

5tas. Jornadas Regionales de Software Libre

5 Jornadas Regionales de Software Libre



Llamado a convocatorias de charlas y posters. !

Mas información en: ***jornadas.ant.org.ar***

Organizan

ANT: www.ant.org.ar
CAFELUG: www.cafelug.org.ar
GLEDUCAR: www.gleducar.org.ar
GRULIC: www.grulic.org.ar
LUGAR: www.linux.org.ar
LUGFI: www.lugfi.org.ar
LUGRO: www.lugro.org.ar
LUGLI: www.lugli.org.ar
LUGMEN: www.lugmen.org.ar
SOLAR: www.solar.org.ar
UYLUG: www.uylug.org.uy
VIA LIBRE: www.vialibre.org.ar

Breves

Cisco no deja escapar el negocio RFID

19/09/2005 - Cisco Systems, fiel a su filosofía de innovación, ultima el lanzamiento de Intelligent Foundation, su gama de productos y servicios RFID para la cadena de suministro. El objetivo de la compañía que lidera John Chambers es simplifica el salto de las compañías a las tecnologías RFID, por lo que el componente de servicios jugará un papel crucial. Tanto es así que prestará soporte a productos de algunos de sus partners como Intermec Technologies, ConnecTerra, ThingMagic y PanGo Networks.
A ello es preciso sumar los servicios que la propia Cisco provee para el despliegue de la red de radiofrecuencia, el desarrollo y puesta en marcha de pilotos y todo el soporte a la implementación de puesta en producción.
El buque insignia de su oferta en este campo es Cisco AON, que cuenta con diferentes módulos con los que introducir la RFID en la cadena de suministro, incorporando prestaciones como la firma digital, la encriptación o el direccionamiento basado en documentos cuando se comparten documentos con partners externos a la organización.
Ya el pasado mes de junio, la multinacional lanzó al mercado norteamericano su dispositivo Cisco 2700, con capacidades inalámbricas (IEEE 802.11) para activar hasta 1.500 etiquetas RFID. A Europa llegará presumiblemente el mes que viene, siendo el mercado asiático el último en recibirlo, ya para la segunda mitad de 2006.

Microsoft y Cisco, una alianza por la seguridad

Para entregar a sus clientes soluciones que ayuden a resolver de una mejor forma las crecientes amenazas y el impacto del software malicioso, Microsoft y Cisco Systems establecieron una alianza que contempla compartir e integrar sus respectivas tecnologías de seguridad y de garantía de salud.
Bajo esta alianza, ambas empresas compartirán información sobre sus tecnologías para poder dirigir un enfoque de compatibilidad de soluciones entre Microsoft Network Access Protection (NAP) y Cisco Network Admissions Control (NAC), que son sus respectivos enfoques de cumplimiento con las políticas de salud y seguridad finales cuando tienen acceso a los recursos de red. Así, las compañías trabajarán para lograr la interoperabilidad entre las arquitecturas NAC y NAP, a medida que estas soluciones evolucionan y son entregadas a los clientes. Este enfoque coordinado permitirá a los clientes integrar las capacidades incorporadas de seguridad de la infraestructura de red de Cisco con las de Windows de Microsoft, permitiéndoles elegir componentes al mismo tiempo que implementan una sola solución integrada.
Este anuncio complementa los exitosos esfuerzos conjuntos de Microsoft y Cisco en un número de diversas alianzas similares y segmentos del mercado, incluyendo arquitecturas de centros de datos, telefonía IP, IPv6, redes y medios para el hogar, y soluciones y programas de canal para las pequeñas y medianas empresas. La seguridad es una extensión importante de esta colaboración y, en esta área, ambas compañías ya han trabajado en conjunto en la tecnología, como en Virtual Private Networks (VPN) y seguridad inalámbrica.

Cisco despacha medio millón de Routers de Servicios Integrados

San José, California, 7 de Octubre de 2005 - Cisco Systems anunció hoy que acaba de despachar su Router de Servicios Integrados número 500.000 a Pep Boys, la cadena de tiendas de repuestos y servicios automotrices más grande de los Estados Unidos. Pep Boys utilizará esta tecnología de redes de avanzada para reducir el tiempo de las transacciones y mejorar su servicio de atención al cliente.
Este anuncio marca un hito en la historia de Cisco: el crecimiento más rápido de un producto desde que fuera lanzado al mercado.
"Desde que Cisco introdujo el portafolio de Routers de Servicios Integrados hemos visto una gran demanda por parte de nuestros clientes alrededor del mundo. Los usuarios se están dando cuenta de que con el uso de estos nuevos routers sus costos y tiempo de instalación e implementación se reducen entre un 40 y un 50 por ciento", dijo Ian Pennell, vicepresidente senior de la Unidad de Negocios de Acceso en Cisco. "En menos de un año Cisco despachó 500.000 routers a miles de clientes de todos los tamaños en mercados e industrias verticales tales como retail, salud, bienes raíces, automotriz, financiero, gobierno y educación. Este gran dinamismo fortificó el liderazgo de Cisco en el mercado global de routing."
A Cisco le tomó seis meses despachar sus primeros 100.000 Routers de Servicios Integrados, y otros seis meses en despachar 500.000. Esta rápida adopción prueba que las organizaciones quieren integrar seguridad, voz y servicios inalámbricos dentro de sus redes, manteniendo al mismo tiempo altos niveles de desempeño, lo que les permite proteger, optimizar y mejorar sus negocios y, al mismo tiempo, invertir para necesidades futuras.



Este logro demuestra el compromiso que Cisco tiene en satisfacer las necesidades de sus clientes. Los Routers de Servicios Integrado de Cisco son los primeros de la industria en proveer a clientes de todos los tamaños servicios de voz, video y datos rápidamente y altamente seguros" señaló Zeus Kerravala, analista de Yankee Group. "Ellos satisfacen las crecientes demandas de los clientes que buscan una red más flexible, sencilla de implementar y eficiente desde el punto de vista de los costos.

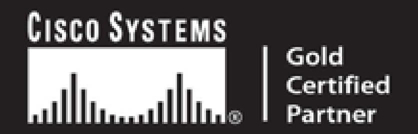
Humor.



Cita...

-"Magia es cualquier tecnología suficientemente avanzada."

Arthur C. Clarke.-



Integramos desde hace 25 años
las mejores soluciones de comunicaciones
y tecnología informática.

Más de 30 profesionales
certificados en tecnologías Cisco:

- 4 CCIEs
- 4 CCNPs
- 4 CCIPs
- 2 CCSPs
- 2 CCDPs
- 25 CCNAs
- 13 CCDAs
- 8 CSEs

Nuestras especializaciones:

- Wireless LAN
- IP Communications
- VPN Security
- Routing & Switching
- ATP Service Control
- Universal Dial Access
- Content Networking

Cisco Gold Certified Partner



Av. Leandro N. Alem 855 - piso 25 - C1001AAD - Buenos Aires - Argentina
Tel.: (54 11) 4590 3600 - Fax.: (54 11) 4590 3601
info@transistemas.com.ar - http://www.transistemas.com.ar

CONTENT DELIVERY NETWORK™
RED DE DISTRIBUCION DE CONTENIDOS

LOAD BALANCING & CONTENT ACCELERATION
BALANCEO DE CARGA Y ACELERACION DE CONTENIDOS

C4™ CONTROL PANEL
PANEL DE CONTROL C4™

99,7% SLA
99,7% UPTIME GARANTIZADO

24/7 PROFESSIONAL SUPPORT
SOPORTE TECNICO PROFESIONAL 24/7

Superamos nuestros propios límites



+54 (11) 5236.7070
www.elserver.com